

RFID

RECHTLICHE DIMENSIONEN
DER RADIOFREQUENZ-IDENTIFIKATION

DIE AUTOREN



Prof. Dr. Bernd Holznagel, LL.M.
Direktor des Instituts für Informations-,
Telekommunikations- und Medien-
recht an der Westfälischen-Wilhelms-
Universität Münster



Mareike Bonnekoh
Wissenschaftliche Mitarbeiterin
am selben Institut

RFID

RECHTLICHE DIMENSIONEN
DER RADIOFREQUENZ-IDENTIFIKATION



SEHR GEEHRTE DAMEN UND HERREN,

RFID ist eine Technologie mit großem Potenzial für Wirtschaft und Verbraucher. Im wirtschaftlichen Bereich liegen die Vorteile vor allem in Effizienzsteigerungen materialwirtschaftlicher und logistischer Prozesse sowie in der Produktionssteuerung und im Zugangsmanagement. Für den Verbraucher bietet die Technologie eine höhere Produktsicherheit, beispielsweise durch eine bessere Rückverfolgbarkeit von Lebensmitteln oder durch den Schutz von Medikamenten gegen Fälschungen.

Noch hat RFID nur punktuell Einzug im Verbraucheralltag gefunden. Szenarien wie der „intelligente Kühlschrank“, in denen Gegenstände via RFID miteinander kommunizieren, sind noch Zukunftsmusik. Auch die Einführung im Einzelhandel findet auf Artekelebene heute zunächst nur im Rahmen einzelner Pilotprojekte statt. Die öffentliche Diskussion zeigt jedoch, dass bei RFID ein Informationsdefizit und darauf basierend vereinzelt auch Unsicherheit besteht.

Die vorliegende Untersuchung über die rechtlichen Dimensionen der Radiofrequenz-Identifikation, die das Informationsforum RFID e. V. in Auftrag gegeben hat, stellt die datenschutzrechtlichen Grundlagen dar und zeigt Wege zu einem verantwortungsvollen Umgang mit der RFID-Technologie auf. Hierdurch soll eine sachliche und zielgerichtete Diskussion ermöglicht werden, die wiederum die Basis dafür ist, dass sowohl Wirtschaft wie auch Verbraucher von den Vorteilen der RFID-Technologie profitieren können.

Die Grundsätze im Bereich der Datenverarbeitung sind gestern und heute dieselben, denn RFID ist lediglich eine neue Form der Datenübermittlung, bei der Daten kontaktlos übertragen werden. Das existierende Datenschutzrecht ist technologieneutral und schafft klare Regeln für die Verarbeitung, Erhebung und Nutzung personenbezogener Daten. Danach gilt: Wenn mithilfe von RFID-Lösungen personenbezogene Daten gespeichert werden, kann dies nur mit Einwilligung des Betroffenen erfolgen.

In der umfassenden Analyse der datenschutz- und datensicherheitsrechtlichen Aspekte von RFID kommt die vorliegende Studie zu dem Ergebnis, dass das geltende Recht in Deutschland ein hohes Schutzniveau für Datenschutz und Datensicherheit garantiert; zusätzliche gesetzliche Regelungen für die RFID-Technologie sind derzeit nicht erforderlich. Wichtig sind jedoch auch die Eigeninitiative und Kooperationsbereitschaft von Wirtschaft, Wissenschaft und Politik. So haben sich beispielsweise die Mitglieder von EPCglobal, einer von Unternehmen getragenen internationalen Organisation für Standardisierung im Bereich RFID, in einer freiwilligen Selbstverpflichtungserklärung auf Grundsätze für den Verbraucherschutz bei der Anwendung von RFID verpflichtet, die beispielhaft sind und über gesetzliche Anforderungen hinausgehen. Ähnliche Aktivitäten gibt es in Deutschland z.B. im Rahmen eines vom Bundeswirtschaftsministerium unterstützten Runden Tisches mit Vertretern aus Handel und Konsumgüterindustrie sowie Daten- und Verbraucherschützern.

Bei allen Diskussionen um RFID sollte man nicht erwarten, schon heute alle Fragen – gleichgültig ob aus technischer oder Datenschutz-Sicht – vollständig zu klären. Dies wird nur anhand konkreter Anwendungen möglich sein. Eine wesentliche Voraussetzung für die Durchsetzung von RFID im Alltag ist jedoch die Akzeptanz der Verbraucher in Bezug auf diese neue Technologie. Das setzt sowohl Vertrauen in die Sicherheit wie auch Transparenz hinsichtlich der Datenverarbeitung voraus. Hierzu will diese Veröffentlichung einen Beitrag leisten.



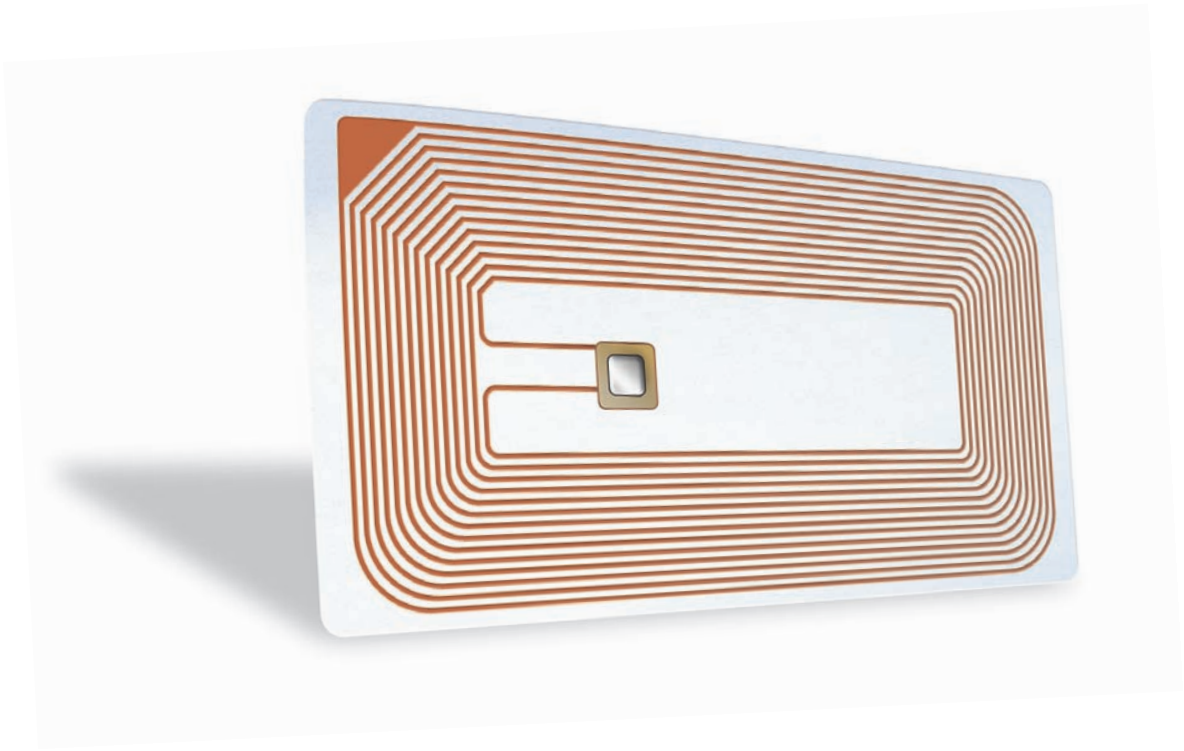
Dr. Andrea Huber

Geschäftsführerin Informationsforum RFID

INHALT

I. Einführung	08
II. Technische Grundlagen von RFID	10
1. Technologische Komponenten von RFID-Systemen	10
2. Energieversorgung	10
3. Frequenzen	11
4. Reichweite von RFID-Tags	12
5. Speicherkapazitäten	13
III. Anwendungsfelder	14
1. Wirtschaft	14
a) Handel	14
b) Verkehr und Automobilindustrie	15
c) Pharmazeutische Industrie	15
2. Öffentliche Einrichtungen und Verwaltung	16
a) Bibliotheken	16
b) Gesundheitswesen	16
c) ÖPNV	17
d) Freizeit	17
e) Reisepässe	17
f) Tierkennzeichnung	18
g) Mauterfassung	18
h) Militär	18
3. Forschung und Entwicklung	19
4. Zugangskontrolle	19
IV. Rechtliche Bewertung von RFID	20
1. Recht des Datenschutzes	20
a) Anwendbarkeit des Datenschutzrechts	21
aa) Speicherung eines Produktcodes auf dem Tag	21
bb) Verknüpfung des Produktcodes mit personenbezogenen Daten	23
cc) Speicherung von personenbezogenen Daten direkt auf dem Tag	24
dd) Fazit	24
b) Datenschutzrechtliche Grundlagen	25
aa) Das Recht auf informationelle Selbstbestimmung	26
bb) Das Verbot mit Erlaubnisvorbehalt	26
cc) Transparenzgebot	26
dd) Zweckbindung	27
ee) Prinzip der Erforderlichkeit	28
ff) Grundsatz der Datensparsamkeit	28
c) Die Phasen des Datenumgangs	28
aa) Erheben	28
bb) Verarbeiten	29
cc) Nutzen	30
d) Einwilligungsvorbehalt gem. § 4 Abs. 1 BDSG	30
e) Ausnahmetatbestände nach § 28 BDSG	32
aa) Zweckbestimmung des Vertrags	32
bb) Wahrnehmung berechtigter Interessen	33
cc) Allgemein zugängliche Quellen	34
f) Sondervorschriften für mobile Speichermedien	34
aa) Anwendungsbereich	34
bb) Unterrichtungspflichten	36
g) Verstoß gegen datenschutzrechtliche Vorschriften	36
h) Fazit	36

2. Recht der Datensicherheit	38
a) Gefahren für die Datensicherheit	38
aa) Abhören der Kommunikation	38
bb) Fälschung des Inhalts oder der Identität	39
cc) Störung des Datenaustauschs	40
dd) Angriff auf das Backend	41
b) Technische Sicherheitsmaßnahmen	41
aa) Authentifizierung	41
bb) Verschlüsselung	42
cc) Verhinderung des Auslesens durch Blocker-Tags	42
dd) Deaktivierung durch Kill-Befehl	43
c) Rechtliche Verpflichtungen zur Sicherung personenbezogener Daten	43
aa) Anforderungen des BDSG	43
bb) Die Anlage zu § 9 BDSG	44
cc) Bedeutung für RFID-Systeme	45
d) Strafrechtlicher Schutz	46
aa) Datenveränderung, § 303a StGB	46
bb) Computersabotage, § 303b StGB	47
cc) Fälschung beweiserheblicher Daten, § 269 StGB	47
dd) Verändern beweiserheblicher Daten, § 274 Abs. 1 Nr. 2 StGB	49
ee) Computerbetrug, § 263a StGB	49
e) Fazit	50
3. Schutz der vertraulichen Kommunikation (Fernmeldegeheimnis)	51
a) Abhörverbot nach § 89 TKG	51
aa) § 89 S. 1 TKG	52
bb) § 89 S. 2 TKG	54
b) Strafbarkeit gem. § 148 Abs. 1 Nr. 1 TKG	54
aa) Objektiver Tatbestand	54
bb) Subjektiver Tatbestand	54
cc) Versuchstrafbarkeit und Vollendung	54
dd) Konkurrenzen und Strafraumen	55
c) Ausspähen von Daten, § 202a StGB	55
aa) Tatobjekt	55
bb) Taterfolg	56
d) Fazit	56
V. Rechtspolitische Debatte	57
1. Technologischer Wandel und das Prinzip der Verantwortung	57
2. Hohes Schutzniveau durch bestehende rechtliche Vorkehrungen	58
3. Optimierung des Schutzinstrumentariums	58
a) Kennzeichnung von Produkten mit RFID	59
b) Auskunft über gespeicherte Informationen	59
c) Deaktivierung von Tags und Verhinderung ihres Auslesens	60
d) Auditierung und Gütesiegel	60
e) Selbstverpflichtungserklärungen	61
4. Zukünftige Entwicklung	62
VI. Zusammenfassung	65
Literaturverzeichnis	67
Internetdokumente	70



I. EINFÜHRUNG

RFID ist die Abkürzung für „**Radiofrequenz-Identifikation**“ und bezeichnet Verfahren zur automatischen und kontaktlosen Identifizierung von Objekten per Funk. RFID-Systeme könnten sich zu einer Schlüsseltechnologie der Zukunft entwickeln und werden schon heute in vielen Bereichen, insbesondere im Logistikbereich und der Lagerbewirtschaftung, nutzbringend eingesetzt. Die Datenübertragung erfolgt durch magnetische oder elektromagnetische Felder.¹ RFID-Systeme bestehen aus zwei technologischen Komponenten: einem Transponder² und einem Lesegerät. Die Vorteile der RFID-Technologie liegen in der Möglichkeit, kontaktlos und ohne optische Verbindung Daten zu übertragen, in der Leseschnelligkeit von weniger als 100 Millisekunden³ und in der Langlebigkeit der Mikrochips. Außerdem sind RFID-Systeme nahezu wartungsfrei.

RFID ist keine neue Technologie. Bereits in den 1940er Jahren entstanden erste Abhandlungen über die Technologie, deren praktische Relevanz allerdings gering war.⁴ In den 1960ern gelangten dann die ersten kommerziell genutzten RFID-Systeme auf den Markt. Dabei handelte es sich um einfache 1-Bit-Transponder, die zur elektronischen Warensicherung⁵ eingesetzt wurden, um Diebstähle zu verhindern.⁶ Mit diesen 1-Bit-Systemen konnte lediglich das Vorhandensein oder das Fehlen der Markierung überprüft werden. In den 1970er und 1980er Jahren wurde die RFID-Technologie weiter entwickelt und gelangte z.B. bei der Tierkennzeichnung und in Zugangskontrollsystemen zur Anwendung. In den 1990ern breitete sich der Einsatz der Systeme weiter aus und es wurden Verwendungsmöglichkeiten in Verkehrssystemen, bei Zahlungsvorgängen und anderen Bereichen erschlossen.⁷ In den 2000ern wurde der Anwendungsbereich für die Transpondertechnologie weiter ausgedehnt, was zu einer größeren Produktion und so zu fallenden Stückpreisen führte. Der Stückpreis für die Mikrochips liegt derzeit bei etwa 10 bis 30 Cent. Für das Jahr 2008 wird mit einem Stückpreis von nur noch wenigen Cent gerechnet. Als „magische Schwelle“ für den Einsatz der Technologie auf dem Massenmarkt wird der Wert von einem Cent betrachtet.⁸

1 *Klußmann*, Lexikon der Kommunikations- und Informationstechnik, 2001, S. 829, 897.

2 Der Begriff Transponder setzt sich zusammen aus den Begriffen Transmitter und Responder, vgl. *Lahner*, Datenschutzrechtliche Probleme beim Einsatz von RFID-Systemen, 2004, S. 1.

3 *Association for Automatic Identification and Mobility (AIM)*, What is Frequency Identification (RFID)?, 2004.

4 *Landt*, Shrouds of Time, The History of RFID, 2001, S. 4.

5 Electronic Article Surveillance (EAS).

6 *Landt*, Shrouds of Time, The History of RFID, a. a. O., S. 4.

7 *Landt*, Shrouds of Time, The History of RFID, a. a. O., S. 5.

8 *Wikipedia*, Freie Enzyklopädie, Stichwort: Radio Frequency Identification, S. 4.

II. TECHNISCHE GRUNDLAGEN VON RFID

1. TECHNOLOGISCHE KOMPONENTEN VON RFID-SYSTEMEN

Jedes RFID-System besteht aus zwei technologischen Komponenten, einem Transponder („Tag“) und einem Lesegerät („Reader“). Der Transponder beinhaltet einen elektronischen Mikrochip und eine Antenne zum Empfangen und Senden von Funkwellen.⁹ Er wird in ein Trägerobjekt integriert, z.B. in ein Klebeetikett oder eine Chipkarte. Auf dem Tag können Informationen, wie beispielsweise ein Nummerncode, gespeichert werden. Um diese gespeicherten Daten erfassen zu können, sind spezielle Lesegeräte erforderlich. Ein Lesegerät, auch Reader genannt, setzt sich aus einem Sender, einem Empfänger und einer Antenne zusammen. Außerdem sind die meisten Lesegeräte mit einer Schnittstelle ausgestattet, um die ausgelesenen Daten an ein anderes System weiterleiten und dort verarbeiten zu können. Der Reader sendet in einer festgelegten Frequenz Funksignale aus, die vom Transponder erfasst werden. Dieser sendet dann seine gespeicherten Daten an das Lesegerät, wo sie erfasst und gespeichert werden.

2. ENERGIEVERSORGUNG

Man unterscheidet aktive und passive RFID-Tags. Passive Tags kommen im Gegensatz zu aktiven Transpondern ohne interne Energiequelle aus. Sie werden bei Lesevorgängen mittels einer großflächigen Spule, die als Antenne dient, durch induktive Kopplung vom Lesegerät per Funk mit Energie versorgt. Dazu wird von der Antennenspule des Lesegerätes aus ein starkes elektromagnetisches Feld erzeugt, das an der Empfängerantenne des Transponders eine Spannung generiert.¹⁰ Diese Spannung dient der Energieversorgung des Tags. Die induktive Kopplung ist die derzeit am meisten verwendete Bauweise für RFID-Systeme. Die Menge der gespeicherten Daten ist bei passiven Funkchips wesentlich geringer als bei aktiven Transpondern. Ein weiterer Unterschied liegt in der geringen Sendereichweite.¹¹ Da keine Batterie benötigt wird, ist allerdings das Gewicht des Tags geringer und die Herstellung kostengünstiger. Außerdem haben sie eine längere Lebensdauer. Aktive Tags hingegen werden durch eine Batterie mit Energie versorgt.¹² Die aktiven Transponder befinden sich normalerweise im Ruhezustand und senden keinerlei Informationen aus, sofern nicht von einem Lesegerät ein Aktivierungssignal empfangen wird. Die Batterie dient nicht der Datenübertragung, sondern allein der Energieversorgung des Mikrochips. Zur Datenübertragung wird auch hier die Energie eines elektromagnetischen Feldes eingesetzt.¹³ Aktive Tags besitzen im Verhältnis zu passiven Transpondern eine höhere Sendereichweite, haben aber eine geringere Lebensdauer und sind deutlich teurer.

⁹ *Finkenzeller*, RFID-Handbuch, Grundlagen und Praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten, 3. Aufl. 2003, S. 6 f.

¹⁰ *Finkenzeller*, RFID-Handbuch, a. a. O., S. 22.

¹¹ *Rankl/Effing*, Handbuch der Chipkarten, 4. Aufl., 2002, S. 95.

¹² *Wikipedia*, Freie Enzyklopädie, Stichwort: Radio Frequency Identification.

¹³ *Finkenzeller*, RFID-Handbuch, a. a. O., S. 23.

3. FREQUENZEN

RFID-Systeme können verschiedene Frequenzbänder¹⁴ nutzen. Weltweit haben sich für RFID-Anwendungen die Frequenzbereiche unter 135 kHz, 13,56 MHz und 860–960 MHz für den kommerziellen Einsatz durchgesetzt. Die Wahl des Frequenzbereichs hat vor allem Auswirkungen auf die Sendeeigenschaften und somit auf die Einsatzbereiche eines RFID-Systems.

Bei der Nutzung niedriger Frequenzbereiche besitzen Tags ohne Batterie lediglich eine Reichweite von wenigen Zentimetern. Im Niedrigfrequenzbereich (125–134 kHz) und im Hochfrequenzbereich (13,56 MHz) eignen Transponder sich für Zugangskontrollen, Wegfahrsperrern und Lagerverwaltung. Die Herstellungskosten sind im niedrigen Frequenzbereich am geringsten. Ein weiterer Vorzug der niedrigen Betriebsfrequenz liegt in der besseren Durchdringung einiger Materialien.¹⁵ Auf hohen Frequenzbändern können aktive Transponder aus einer Entfernung von bis zu mehreren Metern ausgelesen werden. Genutzt werden kann hier grundsätzlich das Ultrahochfrequenzband (860–960 MHz), das bevorzugt im Handel genutzt wird, und der Mikrowellen-Bereich 2,45 GHz.¹⁶ RFID-Systeme, die auf höheren Betriebsfrequenzen arbeiten, erreichen einen größeren Datentransfer und sind unempfindlicher gegenüber elektromagnetischen Störfeldern.¹⁷ Die Auswahl des Frequenzbereichs hängt daher entscheidend davon ab, auf welchem Gebiet das RFID-System eingesetzt werden soll. Das zentrale Problem für die Entwicklung von international einsetzbaren RFID-Systemen liegt in der Frequenzregulierung, da hierfür weltweit uneinheitliche Vorschriften gelten. Unterschiedliche Vorgaben existieren z.B. bei den Zuteilungsregeln der Frequenzbänder und bei der Sendestärke von Lesegeräten.¹⁸ Mittlerweile hat die International Organization for Standardization (ISO) für den Bereich der Transpondertechnologie mehrere Normen verabschiedet.¹⁹ Die ISO-Standards legen Frequenzen, Übertragungsgeschwindigkeiten, Protokolle und Kodierungen fest. Auf europäischer Ebene ist das European Telecommunications Standards Institute (ETSI) für die Entwicklung von einheitlichen Standards zuständig. Viele RFID-Anwendungen folgen in Europa dem ETSI-Standard EN 302 208.

¹⁴ Zu den einzelnen Frequenzbereichen wird auf die umfassenden Ausführungen der Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Risiken und Chancen des Einsatzes von RFID-Systemen, 2004, S. 28 ff., verwiesen.

¹⁵ Finkenzeller, RFID-Handbuch, a. a. O., S. 13.

¹⁶ Dieser Frequenzbereich wird z.B. für Straßenmaut-Systeme genutzt.

¹⁷ Association for Automatic Identification and Mobility (AIM), What is Frequency Identification (RFID)?, a. a. O., S. 1.

¹⁸ So ist im Bereich 869 bzw. 915 MHz in den USA eine maximale Sendeleistung von vier Watt zugelassen, wohingegen in Europa lediglich 0,5 Watt gestattet sind. Dies hat einen erheblichen Unterschied in der Reichweite trotz gleicher Bauweise zur Folge. Sie beträgt in Europa nur bis zu 2,5 Meter, während die Reichweite in den USA zwischen sechs und acht Metern liegt; hierzu BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 30.

¹⁹ Für den Handel sind insbesondere folgende Standards relevant: ISO 1800-6b, ISO 1800-6c und ISO 15693.

4. REICHWEITE VON RFID-TAGS

RFID-Tags verfügen über unterschiedliche Sendereichweiten, die in drei Kategorien eingeteilt werden können: „Close-Coupling“, „Remote-Coupling“ und „Long-Range-Systeme“.²⁰ Die im Folgenden näher angegebenen Reichweiten beziehen sich auf aktive Lese- und Schreibvorgänge.

Close-Coupling-Systeme verfügen lediglich über eine Sendereichweite von bis zu einem Zentimeter. Aufgrund dieser geringen Reichweite muss ein Tag genau positioniert werden, um ausgelesen werden zu können. In der Regel wird der Transponder in das Lesegerät eingesteckt oder auf eine dafür vorgesehene Oberfläche gelegt.²¹ Sie eignen sich daher für die Verwendung in kontaktlosen Chipkarten mit Zahlungsfunktion und bei Zugangskontrollen. Close-Coupling-Systeme können mit nahezu beliebigen Frequenzen arbeiten.²²

Der Sendebereich von Remote-Coupling-Systemen kann bis zu einem Meter betragen. Diese Transponder machen etwa 90 % aller verkauften RFID-Systeme aus. Der mögliche Frequenzbereich liegt üblicherweise bei unter 134 kHz und bei 13,56 MHz. Die Frequenz 13,56 MHz ermöglicht eine schnelle Datenübertragung (106 kBits/s) und ist für den Einsatz einfacher Signalverschlüsselungen geeignet.²³ Im Bereich der Chipkarten haben sich hier die ISO-Normen ISO 14443 (Proximity Coupling) und ISO 15693 (Vicinity Coupling) etabliert.

Long-Range-Systeme verfügen bei der Verwendung von aktiven, also batteriegestützten Tags über eine Reichweite von bis zu 30 Metern. In Ausnahmefällen und bei Verwendung eines extrem hohen Frequenzbereichs können auch Reichweiten bis zu einem Kilometer möglich sein.²⁴ Passive Transponder können bis zu einer Entfernung von drei Metern ausgelesen werden. Die Systeme dieser dritten Kategorie arbeiten generell auf hohen Frequenzen (868 MHz und 2,45 GHz).

5. SPEICHERKAPAZITÄTEN

RFID-Systeme können mit unterschiedlichen Speicherkapazitäten ausgestattet sein und lassen sich von „Low-End-“ bis „High-End-Systemen“ einteilen.²⁵ Die Unterschiede reichen von 1-Bit-Transpondern bis zu Mikroprozessoren, deren Speicher bis zu 100 kByte groß sein kann.²⁶

Dem Low-End-Bereich können zunächst die 1-Bit-Systeme zugeordnet werden. 1-Bit-Transponder können lediglich zwei Zustände anzeigen, nämlich das Vorhandensein oder das Fehlen einer Markierung. Diese Technologie reicht für die oben bereits erwähnten EAS-Systeme²⁷ im Rahmen der Diebstahlsicherung völlig aus. Ebenfalls zum Low-End-Bereich gehören die sog. Read-only-Transponder. Read-only-Transponder sind im Gegensatz zu 1-Bit-Transpondern mit einem Mikrochip ausgestattet. Dieser ermöglicht ausschließlich das Auslesen durch ein Lesegerät. Er ist jedoch nicht beschreibbar, da er lediglich einen ROM²⁸-Speicher besitzt. Dieser Speicher besitzt einen fest codierten Datensatz

20 *Finkenzeller*, RFID-Handbuch, a. a. O., S. 22; *Rankl/Effing*, Handbuch der Chipkarten, 4. Aufl., 2002, S. 101.

21 *Finkenzeller*, RFID-Handbuch, a. a. O., S. 22.

22 BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 40.

23 *Lahner*, Datenschutzrechtliche Probleme beim Einsatz von RFID-Systemen, a. a. O., S. 8 m. w. N.

24 BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 40.

25 *Finkenzeller*, RFID-Handbuch, a. a. O., S. 23 ff.

26 *Finkenzeller*, RFID-Handbuch, a. a. O., S. 24.

27 Vgl. oben Fn. 5.

28 Read Only Memory.

von Informationen. Variable Informationen, die mit dem Tag assoziiert werden sollen, müssen in einer Datenbank im Backend²⁹ des Systems gespeichert werden.³⁰ Wird die auf dem Tag gespeicherte Seriennummer ausgelesen, so können die dazugehörigen Informationen aus der Datenbank abgerufen werden. Bei einem ROM-Speicher werden die Daten dauerhaft und unveränderlich gespeichert. Sie können weder elektrisch noch optisch gelöscht oder verändert werden.³¹ In der Herstellung sind Read-only-Transponder kostengünstig und die Chips können aufgrund der einfachen Technologie minimale Ausmaße annehmen. Allerdings unterstützen die Tags wegen der geringen Speicherkapazität keine Antikollisionsverfahren, so dass nie mehr als ein Tag ausgelesen werden kann.³²

Zu den Systemen mittlerer Leistungsfähigkeit gehören die sog. Read-write-Systeme. Diese verfügen über einen beschreibbaren EEPROM³³-Speicher, der elektronisch programmier- und löschar ist.³⁴ Bei dieser Art von RFID-Systemen können einfache Verschlüsselungsverfahren implementiert werden.³⁵ Read-write-Systeme ermöglichen außerdem die Unterstützung von Antikollisionsverfahren, so dass das Lesegerät trotz mehrerer Tags im Sendebereich dazu in der Lage ist, alle einzeln auszulesen. So kann beispielsweise eine Palette mit mehreren Objekten ausgelesen werden, ohne dass die unterschiedlichen Daten dabei miteinander kollidieren.³⁶ Die am häufigsten verwendeten Antikollisionsverfahren basieren auf dem TDMA³⁷-Prinzip. Bei diesem Verfahren wird die gesamte im Frequenzkanal zur Verfügung stehende Übertragungskapazität nacheinander auf die einzelnen Tags aufgeteilt.³⁸

Im Bereich der High-End-Systeme sind primär kontaktlose Chipkarten anzutreffen. Diese verfügen über einen Mikroprozessor und ein Betriebssystem. Zum Teil sind Chipkarten auch mit zusätzlichen kryptografischen Koprozessoren ausgestattet, die einen hohen Sicherheitsstandard gewährleisten können. Die Herstellungskosten für High-End-Systeme sind relativ hoch, so dass sich der Einsatz dieser hochwertigen Systeme nur in geeigneten Anwendungsbereichen (z.B. in Zahlungssystemen) rentiert.

29 Unter Backend versteht man die Datenbestände, mit denen die vom Lesegerät erfassten Daten über weitere Kommunikationskanäle verknüpft werden.

30 BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 30.

31 BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 30.

32 Befinden sich mehrere RFID-Tags im Lesebereich eines Lesegeräts, so überlagern sich deren Signale, da alle Tags eines bestimmten Typs im selben Frequenzbereich senden. Kommt es zu einer solchen Kollision, so kann das Lesegerät keines der Tags identifizieren. Deshalb ist ein Selektionsverfahren erforderlich, das gewährleistet, dass die Chips ihre Informationen einzeln senden, sog. Antikollisionsverfahren, vgl. BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 35; s. hierzu auch *Finkenzeller*, RFID-Handbuch, a. a. O., S. 24.

33 Electrically Erasable Programmable Read Only Memory.

34 *Lahner*, Datenschutzrechtliche Probleme beim Einsatz von RFID-Systemen, a. a. O., S. 10 m. w. N.

35 *Finkenzeller*, RFID-Handbuch, a. a. O., S. 25.

36 *Hascher*, Identifikation mit Mini-Chips, 2003, S. 2.

37 Time Division Multiple Access.

38 BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 35.

III. ANWENDUNGSFELDER

Der Einsatz von RFID-Systemen eignet sich grundsätzlich überall dort, wo automatisch gekennzeichnet, erkannt, registriert, gelagert, überwacht oder transportiert werden muss. Die Anwendungsfelder sind dementsprechend vielfältig.

1. WIRTSCHAFT

a) Handel

Der Einsatz der Transpondertechnologie bietet sich insbesondere im Handel an.³⁹ Einer Studie zufolge ergeben sich für den Handel vor allem zwei Vorteile: Zum einen können die Bestände und damit die Lager- und Kapitalbindungskosten reduziert werden, zum anderen können Personalkosten eingespart werden.⁴⁰ Eines der wichtigsten Anwendungsgebiete von RFID-Systemen betrifft das „Supply Chain Management“. Darunter versteht man ein Netzwerk verschiedener Unternehmen, die ihre Arbeitsabläufe so aufeinander abstimmen, dass die Steuerung und Überwachung der Lieferkette eines Produkts vom Hersteller bis zum Endkunden optimiert wird.

Im Bereich Lagermanagement dient die RFID-Technologie dem Warenflusssystem, das identifiziert, welche Produkte sich im Lager befinden und welche in den Verkaufsraum verräumt wurden. Aber auch im Endkundenbereich selbst bieten sich für RFID viele Anwendungsfelder. Die RFID-Chips stellen hier vor allem eine Weiterentwicklung der bisherigen Barcodes dar, die jeder Verbraucher z.B. aus dem Supermarkt kennt, wo Barcodes auf den Produkten angebracht sind. Der Strichcode⁴¹ ist eine maschinenlesbare Schrift, die aus Strichen und Lücken unterschiedlicher Breite besteht. Sie kann über optische Abtaster, auch Scanner genannt, maschinell gelesen werden und in einer EDV weiterverarbeitet werden.⁴² Dieselbe Funktion erfüllen auch RFID-Systeme im Handel, nur dass die Funkchips kontaktlos ausgelesen werden können. Ebenso wie beim Barcode wird auch auf einem RFID-Chip lediglich ein Produktcode gespeichert, hier allerdings in elektronischer Form. Daher wird er auch elektronischer Produktcode (EPC) genannt.⁴³ Wird er an der Kasse ausgelesen, so wird der Code mit den entsprechenden Produktdaten in der Produktdatenbank abgeglichen.

Mithilfe der Transponder sind z.B. „intelligente“ Regale möglich, die melden, wann ein mit einem RFID-Chip versehenes Produkt das Regal verlässt und wann neue Ware nachgeräumt werden muss. Den Kunden erwarten außerdem einige Service-Neuheiten. Auf den Tags können zusätzliche Informationen abgespeichert werden, die der Kunde durch ein Lesegerät am Einkaufswagen zur Kenntnis nehmen kann.⁴⁴ Dadurch erhält der Verbraucher weitere Produktinformationen und Empfehlungen zu anderen Waren, die zu dem gesuchten Produkt passen. Auch die Preise können elektronisch im Einkaufswagen erfasst werden, wodurch die bisherige manuelle Barcode-Erfassung entfällt. Entwickelt wurde ferner ein intelligenter Kühlschrank. In dessen Regalböden sind Lesegeräte eingebaut,

39 So wird RFID z.B. im METRO Future Store auf seine Praxistauglichkeit getestet. Die METRO Group Future Store Initiative ist eine Kooperation der METRO Group mit SAP, Intel, IBM und T-Systems sowie weiteren Partnerunternehmen und bildet das Pilotprojekt für Supermärkte mit einem Bündel von technologischen Neuerungen, insbesondere dem Einsatz der RFID-Technologie. Weitere Informationen hierzu unter <<http://www.future-store.org>>.

40 A. T. Kearny: RFID spart dem deutschen Einzelhandel sechs Milliarden Euro pro Jahr. Nutzen für Händler – Kosten für Hersteller, Pressemitteilung vom 08. März 2004, abrufbar über die Homepage der Unternehmensberatung <<http://www.atkearny.de>>.

41 Engl. barcode, bar = Strich.

42 Näher zum Barcode s. Anhang 1.

43 Näheres zum EPC unter IV. 1. a) aa).

44 *Roßnagel/Müller*, CR 2004, 625, 626 f.

die anhand von RFID-Chips erkennen, wann das Mindesthaltbarkeitsdatum eines Produkts abläuft und welche Lebensmittel nachbestellt werden müssen.⁴⁵

RFID-Chips können auch i.V.m. Kundenkarten⁴⁶ verarbeitet werden und dienen hierbei ähnlich wie ein Magnetstreifen oder Barcode als Datenträger. Es können persönliche Daten auf dem Chip gespeichert werden oder auch nur die Kundennummer, die dann in einer Datenbank mit den dort gespeicherten Kundendaten verbunden wird.

b) Verkehr und Automobilindustrie

Seit mehreren Jahren haben sich RFID-Systeme bereits im Bereich der Wegfahrsperrn von Kraftfahrzeugen bewährt. Dabei wird entweder die Zündung, der Anlasser oder die Treibstoffzufuhr unterbrochen. Über ein RFID-Tag im Autoschlüssel kann die Wegfahrsperrre deaktiviert werden.⁴⁷ Das Lesegerät befindet sich im Zündschloss. Ein Kurzschließen des Fahrzeugs ist nicht mehr möglich.

Airbags können bei Autounfällen mit Kleinkindern auf dem Beifahrersitz zu Verletzungen führen. Daher wurde ein Kindersitz mit RFID-Chip entwickelt. Wird der Sitz installiert, so erkennt ein Lesegerät im Auto dies und sendet eine entsprechende Information an die Bordelektronik. Bei einer Kollision wird der Airbag dann nicht vollständig aufgepumpt.⁴⁸

Im Bereich der Luftfahrt kann die Transpondertechnologie bei der Gepäckabfertigung eingesetzt werden. Beim Einchecken des Passagiers wird jedes Gepäckstück mit einem Chip versehen, so dass die Beförderung der Gepäckstücke durch Lesegeräte im Flughafen gesteuert und verfolgt werden kann. Die Lesegeräte erfassen die Transponder entlang des gesamten Transportweges, wodurch weniger Gepäckstücke verloren gehen.

c) Pharmazeutische Industrie

In der Arzneimittelindustrie können RFID-Systeme verwendet werden, um Medikamente leichter zu lokalisieren und Fälschungen und Verluste zu vermeiden bzw. festzustellen.⁴⁹ Die US-amerikanische Behörde Food and Drug Administration (FDA) empfiehlt den Einsatz von RFID-Transpondern, um Produktfälschungen zu verhindern.⁵⁰

45 Vgl. <<http://www.liebherr.com>>.

46 Auf der im METRO Group Future Store verwendeten Kundenkarte, sog. „Future Card“, war zunächst die jeweilige Kundennummer gespeichert, die dann über eine Datenbank mit den jeweiligen Kundendaten verknüpft werden konnte. Seit 2004 werden Kundenkarten mit integriertem RFID-Chip im Rahmen dieses Projekts jedoch nicht mehr eingesetzt.

47 BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 81.

48 Siehe unter <<http://www.daimlerchrysler.com>>.

49 Der US-Pharmakonzern Pfizer setzt z.B. auf die RFID-Technologie, um das Potenzmittel Viagra leichter identifizierbar zu machen und so den Vertrieb von Fälschungen, die derzeit in hoher Zahl auf den Markt strömen, zu erschweren. Ausführlich dazu heise online, Meldung vom 7.1.2006, abrufbar unter <<http://www.heise.de/newsticker/meldung/68093>>.

50 S. unter <<http://www.fda.gov>>.

2. ÖFFENTLICHE EINRICHTUNGEN UND VERWALTUNG

a) Bibliotheken

Einige Bibliotheken haben ihr Ausleihsystem auf RFID umgestellt. Die Medien werden dabei mit Transpondern ausgestattet, wodurch der Ausleihvorgang erheblich beschleunigt wird. Zudem sind die Bücher besser vor Diebstahl geschützt und die Durchführung von Inventuren wird überflüssig. Zu den Bibliotheken, die RFID-Systeme bereits verwenden, zählen u. a. die Wiener Hauptbibliothek⁵¹, die Stadtbüchereien München⁵², Stuttgart⁵³ und Siegburg⁵⁴ sowie die Bücherei des Vatikans⁵⁵.

b) Gesundheitswesen

Auch im Gesundheitswesen finden RFID-Systeme Anwendung. In Krankenhäusern können die Patienten mit einem Transponder, der in ein Armband integriert ist, versehen werden, um die Identität und die Behandlung feststellen und Verwechslungen vermeiden zu können.⁵⁶ Außerdem kann die Auslastung der medizinischen Geräte mithilfe der Patientenarmbänder besser geplant werden. Auf dem Transponder wird die Patientennummer gespeichert. Diese kann der behandelnde Arzt mit einem Personal Digital Assistant (PDA) auslesen und über das lokale Funknetzwerk eine verschlüsselte Verbindung zum Zentralcomputer des Krankenhauses herstellen. So kann dem Arzt die Krankengeschichte des Patienten angezeigt werden. Tags können auch auf dem Operationsmaterial angebracht werden, um sicherstellen zu können, dass am Ende einer Operation nichts im Körper des Patienten vergessen wurde.⁵⁷ Der Einsatz der RFID-Technologie hilft, die Behandlung der Patienten zu verbessern und Verwaltungskosten zu reduzieren. Darüber hinaus kann RFID in Krankenhäusern zur Kontrolle von Blutkonserven und Medikamenten genutzt werden. Auch die Überwachung der Reinigung von Wäsche sowie die Wartung von Betten sind Beispiele der vielfältigen Anwendungsmöglichkeiten.

51 Vgl. unter <<http://buechereien.wien.at>>.

52 S. unter <http://www.muenchner-stadtbibliothek.de/page.php?pageid=1&na_id=1589>.

53 Näheres dazu unter <<http://www.ekz.de/2173.html>>.

54 Vgl. unter <<http://www.siegburg.de/cms124/aktuelles/nachrichten/2001/09/9169/index.html>>.

55 Vgl. heise online, Meldung vom 8.7.2004, abrufbar unter <<http://www.heise.de/newsticker/meldung/48943>>; siehe auch unter <http://bav.vatican.va/en/v_home_bav/home_bav.shtml>.

56 So beispielsweise das Klinikum Saarbrücken in einem Pilotprojekt, näher dazu unter <<http://www.klinikum-saarbruecken.de/kliniknews/index.php3?tid=256&a=NEWS>>.

57 Die amerikanische Gesundheitsbehörde hat sogar eine Genehmigung für den Einsatz von RFID-Transpondern im menschlichen Körper erteilt: Der sog. „VeriChip“ wird unter die Haut injiziert oder eingepflanzt und soll Ärzten bei Notfällen Auskunft über die Krankengeschichte des Patienten geben (Department of Health and Human Services, Food and Drug Administration, 21 CFR Part 880, Docket No. 2004N-0477, veröffentlicht im Federal Register/Vol. 69, No. 237/10. December 2004/Rules and Regulations).

c) ÖPNV

In einigen öffentlichen Verkehrsnetzen, wie z.B. in London, Helsinki und Peking, wird die RFID-Technologie ebenfalls bereits eingesetzt. Der Kunde bezahlt einfach durch Vorhalten seines aufladbaren Fahrscheins. Der entsprechende Betrag wird automatisch von der Karte abgebucht. Die Chipkarte lässt sich dann an dafür vorgesehenen Automaten mit Bargeld oder Kreditkarten wieder aufladen. Dies führt nicht nur zu einer schnelleren Kundenabfertigung, sondern es können auch Kosten dadurch gespart werden, dass der Ausdruck eines Tickets für einmaliges Fahren entfällt. Weitere Vorteile liegen in der automatischen Tarifberechnung, der einfachen Umstellung von Tarifen und in der Prävention von Schwarzfahrten.⁵⁸

In den Bussen der Stadt Hanau wird seit dem Jahr 2002 das „get>>in-Ticket“ benutzt. Die Fahrgäste führen dieses Ticket beim Ein- und Aussteigen an einem Lesegerät im Bus vorbei. Dadurch wird der Fahrpreis für die jeweilige Strecke ermittelt. Die zu zahlenden Beträge werden dann monatlich vom Konto des Kunden abgebucht. Mit der Karte kann auch in anderen Freizeit- und Kultureinrichtungen in Hanau kontakt- und bargeldlos gezahlt werden, z.B. im Schwimmbad und in einigen Museen.⁵⁹

d) Freizeit

RFID kann auch für Freizeitanwendungen genutzt werden. So werden z.B. bei Marathon-Läufern Mini-Transponder an den Schnürsenkeln der Laufschuhe angebracht, mit deren Hilfe registriert wird, wann ein Läufer einen bestimmten Streckenabschnitt passiert.⁶⁰ Neben der genauen Zeitmessung trägt die RFID-Technologie hier auch zur Betrugsvermeidung bei.

e) Reisepässe

Ferner werden Ausweise in Zukunft mit RFID-Tags ausgestattet. Ein aktuelles Beispiel hierfür ist die auf europäischen Vorgaben beruhende Einführung der neuen „ePässe“. ⁶¹ Am 1. November 2005 hat die Ausgabe der neuen biometriegestützten Reisepässe begonnen, die einen Mikrochip enthalten, auf dem zunächst ein digitales Foto gespeichert wird. Ab März 2007 werden dann zusätzlich in den neuen Pässen zwei Fingerabdrücke gespeichert.⁶² Die neuen Pässe sollen die Fälschungssicherheit der Ausweisdokumente erhöhen und dadurch die organisierte Kriminalität und den internationalen Terrorismus bekämpfen.

58 *Finkenzeller*, RFID-Handbuch, a. a. O., S. 358.

59 Einzelheiten zum „get>>in-Ticket“ unter <<http://www.rmvplus.de>>.

60 S. z.B. unter <<http://www.berlin-marathon.com>>.

61 ePass steht für „elektronischer Pass“. Die Einführung des ePasses geschieht aufgrund der Verordnung (EG) Nr. 2252/2004 des Rates v. 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, ABl. Nr. L 385 v. 29.12.2004, S. 1.

62 Vgl. hierzu die ausführlichen Informationen des Bundesministeriums des Inneren, abrufbar über die Homepage des Ministeriums <<http://www.bmi.bund.de>>.

f) Tierkennzeichnung

Eine weitere praxisrelevante Anwendung der Transpondertechnologie ist die Tierkennzeichnung. In der Nutztierhaltung werden mit Identifikationsdaten ausgestattete Transponder am Tier angebracht oder in das Tier injiziert. Hinsichtlich des Formats des Codes⁶³ und der technischen Übertragung⁶⁴ ist von der ISO eine Vereinbarung getroffen worden. Das Tier erhält eine weltweit einmalige Identifikationsnummer, die aus einer 15-stelligen Zahl besteht, welche sich aus einer dreistelligen Länderkennzahl und einer zwölfstelligen nationalen Tiernummer zusammensetzt.⁶⁵ Die Vorteile liegen hier in der schnellen, automatisierten und elektronischen Identifizierung von Tieren, in der eindeutigen Kennzeichnung sowie in der lückenlosen Verfolgbarkeit von der Geburt bis zum Verkauf des Fleisches. Auch im Bereich der Hundehaltung werden RFID-Tags verwendet. Das nordrhein-westfälische Landeshundegesetz schreibt z.B. die Kennzeichnung von Hunden mittels Mikrochip ab einem Gewicht von 20 kg bzw. ab einer Schulterhöhe von 40 cm vor (§ 4 Abs. 7 LHundG NRW).

g) Mauterfassung

Auch für die Mauterfassung eignet sich die RFID-Technologie. Hierbei werden meist aktive Transponder verwendet, die in Plaketten hinter der Windschutzscheibe integriert sind. Maut-RFID-Systeme arbeiten auf hohen Frequenzen, i.d.R. im Mikrowellen-Bereich 2,45 GHz. In Österreich und in einigen US-Bundesstaaten wird die Technologie in Mautsystemen schon eingesetzt.⁶⁶

h) Militär

Das US-amerikanische Verteidigungsministerium nutzt die Transpondertechnologie zur Verwaltung von Beständen und verlangt von seinen wichtigsten Lieferanten, dass sie ihre Sendungen mit RFID-Chips ausrüsten. Dadurch soll die Steuerung des Nachschubs verbessert werden.⁶⁷ RFID wird außerdem vom US-Militär in Verbindung mit dem Global Positioning System (GPS) getestet. Dadurch ließe sich der Standort von Objekten weltweit genau bestimmen. RFID wurde auch von der NATO mit dem Ziel getestet, die Gefahr eines sog. „friendly fire“ zu verhindern.⁶⁸

63 ISO-Norm 11784.

64 ISO-Norm 11785.

65 BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 67.

66 Näheres unter <<http://www.georgiatolls.com>>.

67 Weitere Informationen dazu unter <<http://www.dod.mil>>.

68 Vgl. <http://news.com.com/NATO+tests+RFID+to+prevent+friendly+fire/2100-11395_3-5904392.html>.

3. FORSCHUNG UND ENTWICKLUNG

RFID wird auch im Bereich der Forschung eingesetzt. Die Precision Forestry Cooperative der Universität Washington setzt RFID-Systeme zur Wachstumsüberwachung von genetisch veränderten Bäumen ein. Die Bäume können mithilfe der implantierten Transponder eindeutig identifiziert und so ihr Wachstum genau festgehalten werden.⁶⁹

An der Universität Würzburg ist es Forschern gelungen, den Lebensweg eines Bienenschwarms mithilfe der RFID-Technologie zu verfolgen. Die Informationen, die in einer Datenbank abgelegt werden, ermöglichen es, das Verhalten von Staaten bildenden Insekten zu untersuchen. So kann z.B. die Bedeutung von Umwelteinflüssen identifiziert werden.⁷⁰

4. ZUGANGSKONTROLLE

Transponder werden außerdem im Bereich der Zugangskontrolle eingesetzt. Sie können als Ausweis für den Zutritt von Gebäuden oder Räumen verwendet werden. Auch Skipässe und Clubmitgliedskarten⁷¹ arbeiten mit der RFID-Technologie.

Populäres Beispiel für den RFID-Einsatz sind ferner die Tickets für die Fußball-WM 2006. Da den rund 40 Millionen Kaufinteressenten lediglich eine Million Karten im freien Verkauf zur Verfügung standen, wurden die Tickets verlost. Das Organisationskomitee Deutschland FIFA Fußball-Weltmeisterschaft Deutschland 2006 (kurz: OK) entschloss sich, die WM-Tickets zu personalisieren. In den Antragsformularen mussten die Interessenten Namen, Anschrift, Geburtsdatum, Nationalität und Personalausweisnummer angeben. Die Erhebung dieser Daten sollte der Gewährleistung der Sicherheit und der Verhinderung des Schwarzhandels dienen.⁷² Die Daten der Ausgelosten wurden in einer FIFA-Datenbank gespeichert. Durch einen Abgleich mit Gewalttäter- und Hooligan-Dateien konnten gewaltbereite Personen von vornherein vom Ticketverkauf ausgeschlossen werden. Die Tickets selbst wurden dann mit einem RFID-Chip ausgestattet, der eine eindeutige Zuordnung zu der jeweiligen berechtigten Person ermöglicht. Durch die Verwendung von RFID-Chips sollten die Tickets zudem fälschungssicher gemacht werden. Die Zugangskontrolle erfolgte durch am Eingang positionierte Drehsperrn mit RFID-Lesegeräten. Zusätzliche Ausweiskontrollen wurden stichprobenartig durchgeführt.

69 Näher zu diesem Forschungsprojekt unter <<http://www.cfr.washington.edu>>.

70 Weitere Informationen unter <<http://www.innovationsreport.de>> und unter <<http://www.uni-wuerzburg.de>>.

71 Eine besondere Idee hatte der Baja Beach Club, ein Nachtclub in Barcelona: Besucher des Clubs können sich hier einen Mikrochip unter die Haut spritzen lassen und dann ihre Getränke über ein Kundenkonto bargeld- und kartenlos bezahlen; Börse unter der Haut, Der Spiegel 23/2004, S. 156.

72 So die Erläuterungen zum Datenschutz auf der FIFA-Homepage, vgl. unter <<http://fifaworldcup.yahoo.com>>.

IV. RECHTLICHE BEWERTUNG VON RFID

Durch Fortschritte in der Informationstechnologie entstehen auch im rechtlichen Bereich neue Herausforderungen. Die Entwicklung neuer Technologien soll das Leben bereichern und Prozesse vereinfachen. Aufgrund der kontaktlosen Auslesbarkeit der RFID-Chips wurde in der öffentlichen Diskussion aber auch die Frage aufgeworfen, ob die Technologie Einschränkungen für das Recht der Bürger auf informationelle Selbstbestimmung mit sich bringt. Verbraucherschützer befürchten, dass gesammelte Daten beliebig miteinander verknüpft werden, ohne dass der Bürger etwas davon erfährt. Das deutsche Recht verfügt jedoch über starke Schutzvorkehrungen zur Wahrung der Privatsphäre. Diese werden im folgenden Abschnitt speziell in Bezug auf RFID näher erläutert (dazu unter 1.). Der zweite Teil beschäftigt sich mit der Datensicherheit von RFID-Systemen (dazu unter 2.). Schließlich soll im dritten Teil der rechtlichen Bewertung auf die rechtlichen Vorkehrungen zum Schutz der vertraulichen Kommunikation und damit des Fernmeldegeheimnisses eingegangen werden (dazu unter 3.). Da sich die Diskussion aufgrund des Verbraucherbezugs vor allem auf den Einzelhandel bezieht, soll dieser Anwendungsbereich verstärkt dargestellt werden.

1. RECHT DES DATENSCHUTZES

In jüngster Zeit ist vermehrt über die datenschutzrechtlichen Auswirkungen des Einsatzes von RFID-Systemen diskutiert worden. Im Zentrum der Debatte standen die Anwendungen im Handel, weil hiervon viele Bürger in ihrer Rolle als Verbraucher betroffen sind. Es stellt sich die Frage, ob das geltende Datenschutzrecht dazu in der Lage ist, die Belange der Betroffenen zu wahren, ohne Innovationspotenziale einzuschränken. Vorab kann festgestellt werden, dass nicht alle Verwendungsmöglichkeiten der gleichen juristischen Bewertung zugeführt werden können; es bedarf vielmehr einer differenzierten Betrachtung.⁷³

⁷³ Holzmagell/Bonnekoh, MMR 2006, 17, 19.

a) Anwendbarkeit des Datenschutzrechts

Das Bundesdatenschutzgesetz (BDSG) soll den Einzelnen vor der Beeinträchtigung von Persönlichkeitsrechten schützen, die durch den Umgang anderer mit seinen personenbezogenen Daten entstehen kann.⁷⁴ Der Anwendungsbereich wird also durch den Begriff der „personenbezogenen Daten“ bestimmt. Wie bereits angedeutet, ist nicht jede Verwendungsart von RFID juristisch gleich zu bewerten, sondern es ist zur Bestimmung des datenschutzrechtlichen Anwendungsbereichs danach zu differenzieren, ob personenbezogene Daten betroffen sind. Grundsätzlich lassen sich hier drei verschiedene Grundvarianten unterscheiden:

- ▶ Zum einen gibt es RFID-Anwendungen, bei denen ausschließlich ein elektronischer Produktcode (EPC) auf den Tags gespeichert wird.
- ▶ In einer anderen Variante werden diese Produktcodes mit Kundendaten verknüpft, die in einer Datenbank gespeichert sind.
- ▶ Drittens ist es auch möglich, dass persönliche Kundendaten direkt auf dem Tag gespeichert werden.

aa) Speicherung eines Produktcodes auf dem Tag

In der ersten zu untersuchenden Sachverhaltsvariante wird auf dem Tag lediglich ein elektronischer Produktcode (EPC) gespeichert, wie es im Einzelhandel zukünftig der Fall sein kann. Beispiele hierfür sind die Nutzung von Mehrwegverpackungen sowie die Kennzeichnung von Waren zur automatischen Erfassung im Kassenbereich.

Der Elektronische Productcode (EPC)

Datenkopf	Partition	Filterwert	Basisnummer	Artikelnummer	Seriennummer
48	2	5	4009418	012894	00000123456
EPC-Version SGTIN-86	Handelseinheit: Karton	Trennung nach siebter Ziffer	Hersteller- identifikation: Tip	Warentyp: Küchentücher mit Strukturprägung	

74 Vgl. § 1 Abs. 1 BDSG.

Angenommen, ein Kunde nimmt in einem Supermarkt einen Joghurtbecher, der mit einem RFID-Tag gekennzeichnet ist, aus dem Warenregal. Auf dem Tag ist ein EPC gespeichert. Der EPC wird an der Kasse ausgelesen. Es findet kein Einsatz von Kunden-, ec- oder Kreditkarten statt. Zu prüfen ist, ob hier personenbezogene Daten erhoben bzw. verarbeitet werden oder anders ausgedrückt, ob der Produktcode an sich ein personenbezogenes Datum ist.

Personenbezogene Daten sind gem. § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener).“⁷⁵ Bestimmt ist eine Person, wenn die Daten mit dem Namen des Betroffenen verbunden sind oder sich aus dem Inhalt bzw. dem Zusammenhang der Bezug unmittelbar herstellen lässt.⁷⁶ In der hier dargestellten Sachverhaltsvariante ist der Name des Kunden nicht mit dem auf dem Tag gespeicherten EPC verbunden und lässt sich auch nicht aus dem Zusammenhang unmittelbar herstellen, da der Kunde seinen Namen überhaupt nicht preisgibt. Fraglich ist aber, ob die Person bestimmbar ist. Für die Bestimmbarkeit kommt es auf die Kenntnisse, Mittel und Möglichkeiten der fraglichen Stelle an.⁷⁷ An einer solchen Bestimmbarkeit fehlt es, wenn diese nicht in der Lage ist, die Daten einer Bezugsperson und damit einer natürlichen Person zuzurechnen. Nur wenn personenbezogene Identifizierungsmerkmale festgestellt werden, welche zur Bestimmung der Identität einer Person geeignet sind, liegt eine Erhebung von personenbezogenen Daten vor.⁷⁸ Kauft eine Person Produkte, die mittels RFID-Technologie gekennzeichnet sind, so sind diese Voraussetzungen nicht erfüllt. Der EPC wird zwar an der Kasse ausgelesen, allein durch das Auslesen wird aber kein Bezug zwischen dem Produktcode und dem jeweiligen Kunden hergestellt. Der Kunde gibt Informationen über seine Person weder bei der Entnahme der Ware aus dem Regal noch bei der Übergabe des Geldes an der Kasse her. Es ist auch nicht nachträglich rekonstruierbar, wer welche Ware gekauft hat. Die Person ist folglich auch nicht bestimmbar, so dass die Vorschriften des BDSG somit nicht anwendbar sind.

75 So die Legaldefinition in § 3 Abs. 1 BDSG, vgl. auch Art. 2a der Datenschutzrichtlinie, Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Nr. L 281 vom 23. November 1995, S. 31.

76 *Gola/Schomerus*, BDSG-Kommentar, 8. Aufl., 2005, § 3 Rn. 9.

77 *Dammann*, in: Simitis, Kommentar zum Bundesdatenschutzgesetz, 5. Aufl., 2003, § 3 Rn. 21; *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 3 Rn. 9.

78 *Schild*, in: Roßnagel, Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, 4.2 Rn. 44.

bb) Verknüpfung des Produktcodes mit personenbezogenen Daten

In der zweiten zu untersuchenden Konstellation wird auf dem Tag wiederum ausschließlich ein Produktcode oder eine Seriennummer gespeichert. Es wird jedoch eine Verknüpfung zu personenbezogenen Daten hergestellt, die in der Regel in einer Datenbank (im sog. Backend) gespeichert sind. Dies ist in verschiedenen praktischen Anwendungsfällen denkbar. Möglich wäre z.B. der Einsatz von RFID-Tags bei Paketdiensten und Verleihsystemen. Um das zuvor genannte Beispiel weiterzuführen, ist auch vorstellbar, dass ein Kunde einen mit einem RFID-Chip gekennzeichneten Joghurtbecher, auf dem ein EPC gespeichert ist, kauft und an der Kasse eine Kundenkarte einsetzt. Bei dieser Sachverhaltsvariante wird der auf dem Transponder gespeicherte Produktcode an der Kasse ausgelesen und mit den entsprechenden Produktdaten, die in einer Datenbank gespeichert sind, abgeglichen. Diese Daten werden für die Abwicklung von Kundenrabatten im Rahmen eines Bonussystems⁷⁹ mit den auf der jeweiligen Karte gespeicherten Kundendaten verknüpft. Neben den Produktdaten werden i.d.R. auch weitere Daten wie Ort, Datum und Uhrzeit des Karteneinsatzes sowie der getätigte Umsatz erhoben.

Auch hier ist der Name des Kunden nicht direkt mit dem auf dem Tag gespeicherten Produktcode und den in der Datenbank abgelegten Produktdaten verbunden. Die Person des Kunden ist folglich nicht durch den Produktcode bestimmt. Fraglich ist aber, ob sie in diesem Fall bestimmbar ist, d.h. ob das Unternehmen mit den ihm normalerweise zur Verfügung stehenden Hilfsmitteln bzw. Informationen dazu in der Lage ist, die Produktdaten einer Bezugsperson zuzuordnen. Der Begriff des Personenbezugs ist insofern relativ, d.h., dasselbe Datum kann je nach Umfang des verfügbaren Zusatzwissens aus Sicht eines Dritten anonym und aus der Sicht eines anderen personenbezogen sein.⁸⁰ Durch den Einsatz der Karte im Zusammenhang mit dem Auslesen des Tags wird ein Bezug zwischen den gekauften Produkten und dem Kunden hergestellt. Es handelt sich somit bei dem Produktcode, wenn er bei gleichzeitigem Einsatz einer Kunden-, ec- oder Kreditkarte ausgelesen wird, um Einzelangaben über sachliche Verhältnisse einer bestimmbar natürlichen Person und folglich um personenbezogene Daten. Die Vorschriften des BDSG finden daher Anwendung.

Auch das folgende Beispiel ist dieser Kategorie zuzuordnen: Die Tickets für die Fußball-WM 2006 waren mit RFID-Tags ausgestattet, auf denen eine eindeutige Kennnummer gespeichert ist.⁸¹ Diese Nummer ist personenbeziehbar, da jeder, der eine Eintrittskarte erwerben möchte, bestimmte Angaben zu seiner Person machen muss, die dann in einer Datenbank der FIFA gespeichert werden.⁸² Die Speicherung der Kennnummer auf dem Tag war vor der Bestellung und Auslosung der Tickets datenschutzrechtlich belanglos. Danach aber konnten sämtliche in der Datenbank erfassten Antragsdaten über die eindeutige Kennnummer erschlossen werden.⁸³

⁷⁹ Derartige Bonussysteme dienen in der Regel der Kundenbindung. Grundlage der Teilnahme an einem Kundenbindungssystem ist ein entsprechender Vertrag des Kunden mit dem Unternehmen. In dem Vertrag verpflichtet sich das Unternehmen, gegenüber dem Kunden Rabatte zu gewähren oder bestimmte Serviceleistungen zu erbringen. Vgl. hierzu das Gutachten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), Kundenbindungssysteme und Datenschutz, 2003, S. 69.

⁸⁰ *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 4. Aufl. 2005, S. 280.

⁸¹ Siehe hierzu bereits oben unter III. 4.

⁸² *Conrad*, CR 2005, 537, 538.

⁸³ *Conrad*, CR 2005, 537, 538.

cc) Speicherung von personenbezogenen Daten direkt auf dem Tag

Werden Angaben über persönliche oder sachliche Verhältnisse einer Person direkt auf einem RFID-Tag gespeichert, so beziehen sie sich auf eine bestimmte Person und unterliegen damit dem Schutz des BDSG. Anzutreffen sind solche Anwendungen überall dort, wo die Integration personenbezogener Daten Voraussetzung ist, also dort, wo es um Identifikation und Sicherheit geht. Dies ist der Fall bei personenbezogenen Daten, die für die Zugangskontrolle für Gebäude erforderlich sind, bei Signaturkarten oder bei Karten mit besonderen Schutzmechanismen. Aktuelle Beispiele hierfür sind ÖPNV-Tickets sowie biometrische Daten, die in den neuen e-Pässen gespeichert werden. Die Einführung dieser Variante ist z.B. im Einzelhandel nicht geplant. Dementsprechend sieht auch die EPCglobal-Selbstverpflichtung⁸⁴ vor, dass auf RFID-Tags keine personenbezogenen Daten gespeichert werden.

dd) Fazit

Zusammenfassend lässt sich also festhalten, dass ein auf einem RFID-Tag gespeicherter EPC für sich betrachtet kein personenbezogenes Datum ist und datenschutzrechtliche Vorschriften folglich nicht anwendbar sind, solange über den EPC keine Verknüpfung zu personenbezogenen Daten hergestellt wird. Findet eine Verknüpfung mit personenbezogenen Daten statt, so ist der Anwendungsbereich des BDSG eröffnet. Die Speicherung von personenbezogenen Daten unmittelbar auf dem Tag führt selbstverständlich ebenfalls zur Anwendbarkeit des BDSG, wird aber derzeit nur selten praktiziert.

84 Das EPCglobal-Netzwerk entwickelt wirtschaftliche und technische Standards für den EPC. Näher dazu unter V. 3. e).

b) Datenschutzrechtliche Grundlagen

Nur wenn bei RFID-Anwendungen personenbezogene Daten betroffen sind, sind die datenschutzrechtlichen Vorschriften zu beachten. Dies ist in der unter aa) geschilderten Sachverhaltsvariante, bei der lediglich ein EPC auf einem Tag gespeichert wird, nicht der Fall. Zum besseren Verständnis der einzelnen Regelungen sollen zunächst einige datenschutzrechtliche Grundlagen dargestellt werden:

aa) Das Recht auf informationelle Selbstbestimmung

In seinem „Volkszählungsurteil“⁸⁵ hat das BVerfG aus dem Grundrecht auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) und der Achtung der Menschenwürde (Art. 1 Abs. 1 GG) das Recht auf informationelle Selbstbestimmung abgeleitet. Dieses beinhaltet die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.⁸⁶ Wer nicht mit Sicherheit überschauen kann, welche Informationen über ihn in seiner sozialen Umwelt bekannt sind, kann in seiner Freiheit gehemmt sein, aus eigener Selbstbestimmung zu planen und zu handeln.⁸⁷ Wer nicht weiß, welche Verhaltensweisen registriert werden, wird versuchen, nicht aufzufallen, und wird dadurch unter Umständen in der Ausübung seiner Grundrechte eingeschränkt. Das Recht auf informationelle Selbstbestimmung macht daher den Einzelnen selbst grundsätzlich zum Herrn über die ihn betreffenden Daten.

Neue Technologien können die Privatsphäre des Einzelnen auf eine Weise berühren, die bei der Ausarbeitung des BDSG so nicht absehbar war. Individuelle Selbstbestimmung muss aber gerade auch unter den Bedingungen moderner Informationstechnologien gewährleistet sein. Entsprechend führt das BVerfG in seinem Urteil weiter aus, dass für jede Person die Möglichkeit bestehen muss, auch unter veränderten technologischen Bedingungen grundsätzlich über die Erhebung, Verarbeitung und Nutzung ihrer Daten zu bestimmen. Es fordert somit eine dynamische Fortschreibung des Grundrechtsschutzes unter Berücksichtigung des technischen Fortschritts.⁸⁸

85 BVerfGE 65, 1 ff.

86 BVerfGE 65, 1, 42.

87 *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 1 Rn. 9.

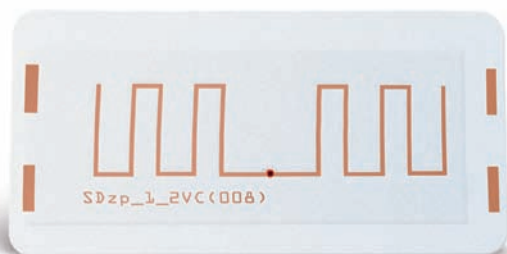
88 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, a. a. O., S. 142.

bb) Das Verbot mit Erlaubnisvorbehalt

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nach dem in § 4 Abs. 1 BDSG niedergelegten Grundsatz des „Verbots mit Erlaubnisvorbehalt“⁸⁹ nur dann zulässig, wenn der Betroffene eingewilligt hat oder das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet. Als Erlaubnistatbestände für das Erheben, Speichern, Übermitteln, Verändern und Nutzen personenbezogener Daten für eigene Zwecke kommen insbesondere die Erlaubnistatbestände des § 28 Abs. 1 S. 1 Nr. 1 und Nr. 2 BDSG in Betracht. Danach ist der Datenumgang zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient (Nr. 1) oder soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (Nr. 2).

cc) Transparenzgebot

Soll der Einzelne selbst entscheiden können, wann und wem er welche Daten preisgibt, so ist hierfür die Transparenz der Erhebungs- und Verarbeitungszusammenhänge notwendig. Dies erfordert vor allem institutionelle Vorkehrungen der Transparenz und Unterrichtung der Betroffenen im öffentlichen wie im privaten Bereich.⁹⁰ Der Betroffene hat ein Recht auf Offenlegung der über ihn gespeicherten Daten. Nur so ist es ihm möglich, evtl. Löschungs- und Korrekturanträge geltend zu machen.⁹¹ Ihm werden daher Auskunftsrechte gewährt (§§ 19a, 34 BDSG). Um von diesen Auskunftsrechten Gebrauch machen zu können, muss der Betroffene von einer Datenerhebung benachrichtigt werden. Es bestehen deshalb Benachrichtigungspflichten der verantwortlichen Stellen (§§ 19, 33 BDSG). Verletzt eine private Stelle eine bestehende Benachrichtigungspflicht, so kann dies als Ordnungswidrigkeit gem. § 43 Abs. 1 Nr. 8 BDSG mit einem Bußgeld belegt werden. Das erforderliche Maß hinsichtlich Art, Gegenstand, Inhalt und Reichweite von Auskunfts- und Benachrichtigungspflichten bemisst sich an dem Ziel, die Transparenz und Nachvollziehbarkeit der Datenerhebungs- und -verarbeitungsvorgänge zu sichern.⁹²



89 Gola/Schomerus, BDSG, Bundesdatenschutzgesetz, Kommentar, a. a. O., § 4 Rn. 3; Globig, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4.7 Rn. 6; Sokol, in: Simitis, Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 4 Rn. 3.

90 Trute, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 2.5 Rn. 33.

91 BVerfGE 100, 313, 361; Gola/Schomerus, BDSG-Kommentar, a. a. O., § 33 Rn. 1.

92 Trute, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 2.5 Rn. 34.

Werden im Zusammenhang mit dem Einsatz von RFID-Systemen personenbezogene Daten erhoben, verarbeitet oder genutzt, sind die verantwortlichen Stellen zur Benachrichtigung des Betroffenen hierüber verpflichtet. Dies gilt allerdings nur, soweit die Datenerhebung ohne Kenntnis des Betroffenen erfolgt, §§ 19a Abs. 1 S. 1, 33 Abs. 1 S. 1 BDSG. Das bedeutet insbesondere, dass, wenn eine Einwilligung für die Erhebung eingeholt worden ist, die Benachrichtigungspflicht entfällt.⁹³ In jedem Fall müssen dem Betroffenen die o. g. Auskunftsrechte gewährleistet werden.

Besondere Bedeutung haben Informations- und Auskunftsrechte dort, wo aufgrund technischer Vorkehrungen das Verhalten von Personen umfassend und unbemerkt dokumentiert werden kann.⁹⁴ Besonders kritisch stellt sich die Situation dar, wenn es sich um sog. sensitive Daten⁹⁵ handelt, beispielsweise wenn RFID im pharmazeutischen oder klinischen Bereich eingesetzt wird.

dd) Zweckbindung

Nach dem Grundsatz der Zweckbindung dürfen personenbezogene Daten nur für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nur für diese Zwecke weiterverarbeitet werden.⁹⁶ Jede zweckwidrige Nutzung ist unzulässig. Insbesondere verstößt nach dem Volkszählungsurteil die Speicherung „auf Vorrat zu unbestimmten Zwecken“ gegen das Recht auf informationelle Selbstbestimmung. Der Zweckbindungsgrundsatz ist im BDSG nicht *expressis verbis* erwähnt, findet aber beispielsweise Eingang in § 14 BDSG, wonach das Speichern, Verändern oder Nutzen personenbezogener Daten nur zulässig ist, wenn es für die Zwecke erfolgt, für die die Daten erhoben worden sind. In der Konsequenz bedeutet dies auch, dass der Erhebung eine Festlegung des Zweckes vorausgegangen sein muss.⁹⁷

⁹³ *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 33 Rn. 8.

⁹⁴ *Trute*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 2.5 Rn. 33 in Bezug auf die Dokumentation des Kommunikationsverhaltens. Aus diesem Grund ist auch für Medien- und Teledienste eine Unterrichtung vor der Datenerhebung vorgesehen (§ 18 Abs. 1 MDStV, § 4 Abs. 1 TDDSG).

⁹⁵ Dabei handelt es sich um Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (besondere Arten personenbezogener Daten), vgl. § 3 Abs. 9 BDSG.

⁹⁶ So die Vorgaben in Art. 6 Abs. 1 Buchst. b der EG-Datenschutzrichtlinie für elektronische Kommunikation, Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. EG L 201 vom 31.07.2002, S. 37.

⁹⁷ *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 14 Rn. 9; *Trute*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 2.5 Rn.

ee) Prinzip der Erforderlichkeit

Der Grundsatz der Zweckbindung wird flankiert vom Erforderlichkeitsgrundsatz.⁹⁸ Dieser bezeichnet die Relation zwischen dem Datenverarbeitungsvorgang und der Sachaufgabe, der sie dient.⁹⁹ Daten dürfen nur dann erhoben und verarbeitet werden, wenn sie für die Bearbeitung der jeweiligen Aufgabe erforderlich sind. Für nicht-öffentliche Stellen hat dieser Grundsatz Eingang in offene Abwägungsklauseln gefunden, so z.B. in § 28 Abs. 1 S. 1 Nr. 1 BDSG: „wenn es der Zweckbestimmung eines Vertragsverhältnisses dient“; und in § 28 Abs. 1 S. 1 Nr. 2 BDSG: „soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist.“ Was dies in der Konsequenz für den Einsatz der Transpondertechnologie bedeutet, wird noch zu erörtern sein.¹⁰⁰

ff) Grundsatz der Datensparsamkeit

Das Prinzip der Erforderlichkeit wird zudem konkretisiert durch den Grundsatz der Datenvermeidung und -sparsamkeit, § 3a BDSG. Danach haben sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten, keine (Datenvermeidung) oder so wenig wie möglich (Datensparsamkeit) personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen (S. 1). Es soll insbesondere von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch gemacht werden (S. 2). Durch diesen „Datenschutz durch Technik“ sollen Gefährdungen des informationellen Selbstbestimmungsrechts präventiv reduziert werden.¹⁰¹ So ist auch bei der technischen Entwicklung von RFID-Systemen darauf zu achten, dass diese so datenschutzfreundlich wie möglich sind.

c) Die Phasen des Datenumgangs

Als Phasen des Umgangs mit personenbezogenen Daten nennt das BDSG das Erheben, Verarbeiten und Nutzen.

aa) Erheben

Erheben ist gem. § 3 Abs. 3 BDSG das Beschaffen von Daten über den Betroffenen. Gemeint ist das gezielte Beschaffen von Daten, so dass die sich zufällig oder in Verbindung mit einer anderen Handlung ergebende Wahrnehmung keine Erhebung darstellt.¹⁰² In der Alltagsanwendung von RFID wird es wahrscheinlich sein, dass bei einer Abfrage durch ein Lesegerät auch andere Tags ungewollt mit erfasst werden. Bei der automatischen Identifikation erfolgt die Erfassung der Kennungen aller RFID-Chips in der Reichweite des Lesegeräts und kann nicht auf bestimmte Tags beschränkt werden.¹⁰³ Passiert z.B. ein Kunde in einem Supermarkt eine RFID-Kasse mit automatischer Erfassung der Ware, so werden möglicherweise auch andere RFID-Tags von Produkten, die der Kunde in einem anderen

98 BVerfGE 65, 1, 43, 46.

99 *Trute*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 2.5 Rn. 43 m. w. N.

100 Siehe unter IV. 1. e).

101 *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 3a Rn. 1.

102 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, a. a. O., S. 296; zur Unterscheidung zwischen zielgerichteter und ungezielter Datenerhebung s. auch unter V. 4.

103 *Müller*, DuD 2004, 215, 217.

Geschäft gekauft hat, zwangsläufig mit ausgelesen.¹⁰⁴ Ein solches nicht zielgerichtetes Auslesen von RFID-Tags ist keine Datenerhebung i.S.d. BDSG. Werden diese Daten dann allerdings weiter verwendet, so finden die datenschutzrechtlichen Bestimmungen Anwendung.¹⁰⁵ Die verantwortliche Stelle darf sich nicht auf sie berufen und darf sie nicht speichern. Sind sie bereits gespeichert, so sind die Daten unverzüglich zu löschen, § 20 Abs. 2 Nr. 1, § 35 Abs. 2 Nr. 1 BDSG.¹⁰⁶

Der Betroffene ist bei der Erhebung nach § 4 Abs. 3 BDSG über die Identität der erhebenden Stelle, die Zweckbestimmungen der Erhebung, Verarbeitung und Nutzung und die Kategorien von Empfängern zu unterrichten. Die Zwecke der Datenerhebung sind von der verantwortlichen Stelle bereits vor der Erhebung festzulegen, § 14 Abs. 1 S. 1 bzw. § 28 Abs. 1 S. 2 BDSG. Außerdem müssen die zu erhebenden Daten für den konkreten Zweck erforderlich sein.¹⁰⁷

bb) Verarbeiten

Verarbeiten ist gem. § 3 Abs. 4 S. 1 BDSG das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Diese fünf Phasen des Verarbeitens sind im BDSG legal definiert. Danach ist Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung.¹⁰⁸ In Abgrenzung zur Datenerhebung setzt die Speicherung voraus, dass das Erfassen, Aufnehmen oder Aufbewahren zum Zwecke der weiteren Verwendung erfolgt. Das BDSG ist bereits dann anwendbar, wenn eine bedingte Verwendungsabsicht vorliegt.¹⁰⁹

Verändern ist das inhaltliche Umgestalten gespeicherter personenbezogener Daten.¹¹⁰ Ein inhaltliches Umgestalten liegt bereits dann vor, wenn durch die Maßnahme der Informationsgehalt einer Nachricht geändert wird, so dass ein neuer Aussagewert entsteht.¹¹¹ Das kann durch die Berichtigung oder Verfälschung von Daten oder durch das Herausnehmen aus dem Zusammenhang oder das Einfügen von Daten in andere Zusammenhänge geschehen.

Übermitteln ist das Bekanntgeben personenbezogener Daten an einen Dritten, und zwar entweder durch Weitergabe der Daten durch die verantwortliche Stelle an den Dritten (a) oder dadurch, dass der Dritte die bereitgehaltenen Daten einzieht oder abrufen (b).¹¹² Dabei kommt es auf die konkrete Einsichtnahme bzw. den konkreten Abruf an.¹¹³

Sperren ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.¹¹⁴ Personenbezogene Daten sind vor allem dann zu sperren, wenn eine Verpflichtung zur Sperrung besteht (§§ 20 und 35 BDSG), wenn ein Widerspruch des

104 Dies führt jedoch nicht zu einer falschen Berechnung, da das Kassensystem erkennen kann, ob es sich um Waren aus dem eigenen Bestand handelt.

105 Hierzu sogleich unter IV. 1. c) bb) und cc).

106 *Schild*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4.2, Rn. 47.

107 *Schild*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4.2, Rn. 52; zum Erforderlichkeitsgrundsatz siehe bereits oben unter IV. 1. b) ee).

108 § 3 Abs. 4 S. 2 Nr. 1 BDSG.

109 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, a. a. O., S. 299.

110 § 3 Abs. 4 S. 2 Nr. 2 BDSG.

111 *Schild*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4.2, Rn. 64; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, a. a. O., S. 300.

112 § 3 Abs. 4 S. 2 Nr. 3 BDSG.

113 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, a. a. O., S. 302.

114 § 3 Abs. 4 S. 2 Nr. 4 BDSG.

Betroffenen vorliegt (§§ 20 Abs. 5, 28 Abs. 4, 29 Abs. 4 und 35 Abs. 5 BDSG), und bei gesonderter Speicherung der Identifikationsmerkmale (§§ 30 Abs. 1 und 40 Abs. 2 BDSG). Die Kennzeichnung muss in technischer Hinsicht bewirken, dass die Daten nur noch eingeschränkt bzw. für gesetzliche Ausnahmefälle verwendet werden können.¹¹⁵

Löschen ist das Unkenntlichmachen gespeicherter personenbezogener Daten.¹¹⁶ Diese Phase beendet die Verarbeitung von Daten.¹¹⁷ Die gespeicherten Daten dürfen nicht mehr rekonstruierbar sein.¹¹⁸ Das Deaktivieren eines RFID-Tags wäre als Löschen der Daten einzuordnen, da der Chip unbrauchbar wird und ein Bezug zu den in der Datenbank gespeicherten Daten nicht mehr hergestellt werden kann. Die Personenbeziehbarkeit wäre in diesem Fall also nicht mehr gegeben.

cc) Nutzen

Nutzen ist gem. § 3 Abs. 5 BDSG jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt. Das Verwenden von Daten kann also als Obergriff für das Begriffspaar „Verarbeiten und Nutzen“ aufgefasst werden.¹¹⁹ Die Nutzung muss sich auf die personenbezogenen Daten beziehen. Eine Nutzung kann z.B. ein Abgleich oder eine statistische Auswertung sein sowie das Erstellen einer Rechnung, das Kopieren von Daten oder die Weitergabe zur Auftragsdatenverarbeitung.¹²⁰ Auch die Verwendung von Informationen innerhalb der verantwortlichen Stelle stellt ein Nutzen i.S.d. Vorschrift dar.¹²¹

d) Einwilligungsvorbehalt gem. § 4 Abs. 1 BDSG

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind vom gesetzlichen Ansatz her verboten. Sie sind aber gem. § 4 Abs. 1 BDSG dann zulässig, wenn der Betroffene eingewilligt hat oder soweit ein gesetzlicher Ausnahmetatbestand den Datenumgang erlaubt. Diesen Grundsatz bezeichnet man auch als „Verbot mit Erlaubnisvorbehalt“.¹²² So ist die Einwilligung z.B. grundsätzlich erforderlich bei Werbemaßnahmen, die die Privatsphäre des Betroffenen tangieren.¹²³ Erlaubnistatbestände können sich sowohl im BDSG selbst als auch in anderen Rechtsvorschriften befinden.

Sollen beim Einsatz von RFID-Systemen personenbezogene Daten erhoben oder verarbeitet werden, so ist hierfür grundsätzlich eine Einwilligung des Betroffenen erforderlich, soweit kein gesetzlicher Erlaubnistatbestand eingreift. Das Einwilligungserfordernis dient der Selbstbestimmung des Betroffenen und stellt zugleich eine Konkretisierung des Transparenzgebots dar: Der Betroffene muss wissen, wann beim Einsatz der RFID-Technologie personenbezogene Daten auf einem Transponder,

115 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, a. a. O., S. 303; zu der Frage, wie dies technisch im Einzelfall realisiert werden kann vgl. Schild, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4,2, Rn. 87.

116 § 3 Abs. 4 S. 2 Nr. 5 BDSG.

117 *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 3 Rn. 40.

118 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, a. a. O., S. 303.

119 *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 3 Rn. 41.

120 *Schild*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4,2, Rn. 87.

121 *Schild*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4,2, Rn. 87; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, a. a. O., S. 306.

122 Dazu auch bereits unter IV. 1. b) bb).

123 *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 4a Rn. 4.

mit dem er in Berührung kommt, gespeichert werden. In der Konsequenz bedeutet dies natürlich auch, dass kein Einwilligungserfordernis und damit auch keine gesetzliche Kennzeichnungspflicht für Transponder besteht, wenn keine personenbezogenen Daten gespeichert werden.¹²⁴

Bei der Einwilligung handelt es sich nach dem Begriffsverständnis des BGB um eine antizipierte Erlaubnis, d.h., dass sie ausnahmslos der Datenverarbeitung vorausgehen muss.¹²⁵ Eine nachträgliche Genehmigung reicht hingegen nicht aus¹²⁶ und macht eine vorausgegangene illegale Datenverarbeitung auch nicht zulässig.¹²⁷ Die datenschutzrechtliche Einwilligung ist als geschäftsähnliche Handlung zu qualifizieren, so dass in zivilrechtlicher Hinsicht die Vorschriften über Willenserklärungen grundsätzlich entsprechend anzuwenden sind.¹²⁸

Das BDSG stellt an die Einwilligung einige formale und inhaltliche Anforderungen. Dadurch soll gewährleistet werden, dass der Betroffene die Tragweite seiner Entscheidung richtig abschätzen kann. So muss die Einwilligungserklärung gem. § 4a Abs. 1 S. 1 BDSG auf der freien Entscheidung des Betroffenen beruhen und grundsätzlich schriftlich erfolgen (S. 3). Eine Einwilligungserklärung, die der Schriftform nicht genügt, ist in entsprechender Anwendung der §§ 125, 126 BGB unwirksam und führt zur Unzulässigkeit der darauf beruhenden Datenverarbeitung.¹²⁹ Eine mündliche Einwilligungserklärung kann nur unter besonderen Umständen als ausreichend betrachtet werden. In diesem Zusammenhang ist eine Abwägung der beteiligten Interessen unter Berücksichtigung der jeweiligen Verarbeitungsumstände vorzunehmen. Zu beachten ist hierbei, dass es sich um eine Ausnahmeregelung handelt, die grundsätzlich restriktiv auszulegen ist.¹³⁰ Zu den Fallgruppen, in denen eine mündliche Einwilligung genügen kann, zählen dauerhafte und langfristige Geschäftsbeziehungen,¹³¹ Eilbedürftigkeit¹³² und Eigeninteresse des Betroffenen.¹³³ Außerdem muss der Betroffene auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung und, soweit dies erforderlich ist oder der Betroffene es verlangt, auf die Folgen der Verweigerung der Einwilligung hingewiesen werden (S. 2).

Oftmals wird die Einwilligung zusammen mit anderen Erklärungen abgegeben. Dies kann insbesondere bei Vertragsabschlüssen den Verwaltungsaufwand reduzieren. In diesen Fällen darf die Einwilligung nicht in anderen Erklärungen „versteckt“ werden. Daher ist sie gem. § 4 Abs. 1 S. 4 BDSG besonders hervorzuheben, wenn sie zusammen mit anderen Erklärungen schriftlich erteilt wird.

124 Zu dem Bedürfnis nach einer Selbstverpflichtung zur Kennzeichnung siehe unter V. 3. a).

125 *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 4 Rn. 15; *Holznapel/Sonntag*, in: *Roßnagel*, Handbuch Datenschutzrecht, a. a. O., 4.8, Rn. 19; zur Rechtsnatur der Einwilligung vgl. auch *Heinrichs*, in: *Palandt*, Einf. vor § 182, Rn. 1 ff.

126 *Schaffland/Wiltfang*, Bundesdatenschutzgesetz, Kommentar, Stand 2005, § 4a Rn. 2.

127 Sie kann allerdings dazu führen, dass Schadensersatzansprüche ausgeschlossen sind, vgl. *Holznapel/Sonntag*, in: *Roßnagel*, Handbuch Datenschutzrecht, a. a. O., 4.8, Rn. 19 m. w. N.

128 *Holznapel/Sonntag*, in: *Roßnagel*, Handbuch Datenschutzrecht, a. a. O., 4.8, Rn. 21 ff.

129 Vgl. *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 4a Rn. 13.

130 *Holznapel/Sonntag*, in: *Roßnagel*, Handbuch Datenschutzrecht, a. a. O., 4.8, Rn. 29.

131 Dies gilt für erneute oder zusätzliche Datenerhebungen, wenn eine schriftliche Einwilligung ursprünglich erteilt worden ist; dazu *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 4a Rn. 13; *Schaffland/Wiltfang*, Bundesdatenschutzgesetz-Kommentar, a. a. O., § 4a Rn. 5; *Simits*, in: *Simits*, Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 4a Rn. 48.

132 Jedoch nur, wenn der Betroffene ein eigenes Interesse daran hat, z.B. bei einem ärztlichen Heileingriff im Notfall, *Schaffland/Wiltfang*, Bundesdatenschutzgesetz-Kommentar, a. a. O., § 4a Rn. 5; *Bergmann/Möhrl/Herb*, Datenschutzrecht, Kommentar zum Bundesdatenschutzgesetz, den Datenschutzgesetzen der Länder und zum Bereichsspezifischen Datenschutz, Loseblattsammlung, Stuttgart, Stand: September 2005, § 4a Rn. 55.

133 Wenn der Betroffene auf eigene Initiative eine Datenverarbeitung wünscht, die die Abgabe einer schriftlichen Einwilligung nicht zulässt, z.B. bei telefonischer Bestellung mit sofortiger Auslieferung, vgl. *Holznapel/Sonntag*, in: *Roßnagel*, Handbuch Datenschutzrecht, a. a. O., 4.8, Rn. 29.

e) Ausnahmetatbestände nach § 28 BDSG

Eine Einwilligung ist dann nicht erforderlich, wenn ein gesetzlicher Ausnahmetatbestand vorliegt. Für den Datenumgang von nicht-öffentlichen Stellen kommen insbesondere die Erlaubnistatbestände nach § 28 BDSG in Betracht. Liegen die Voraussetzungen der jeweiligen Vorschrift nicht vor, so ist die Datenverarbeitung unzulässig. Gespeicherte Daten müssen dann gem. § 35 Abs. 2 S. 2 Nr. 1 BDSG unverzüglich gelöscht werden.

aa) Zweckbestimmung des Vertrags

Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist gem. § 28 Abs. 1 S. 1 Nr. 1 BDSG zulässig, wenn es der Zweckbestimmung des Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient. Durch das Merkmal des vertragsähnlichen Vertrauensverhältnisses wird deutlich, dass bereits im Vorfeld eines Vertrags sowie nach Beendigung des Vertrags eine Speicherung personenbezogener Daten erlaubt sein kann.¹³⁴

Werden im Rahmen eines Vertragsverhältnisses RFID-Systeme eingesetzt und werden dabei personenbezogene Daten gespeichert, so muss die Speicherung der Zweckbestimmung dieses Vertrags dienen, d.h., zwischen der Speicherung und der Abwicklung des Vertrags muss ein unmittelbarer sachlicher Zusammenhang¹³⁵ bestehen. Kauft jemand beispielsweise Waren, dürfen dessen Kundendaten nur im Rahmen der Durchführung des Vertrags gespeichert werden. Die Verwendung der Daten für eine Werbekampagne kann nicht auf den Kaufvertrag und somit nicht auf § 28 Abs. 1 S. 1 Nr. 1 BDSG gestützt werden.¹³⁶ Auch die beim Einsatz von ec- oder Kreditkarten erhobenen Daten dürfen nur für den Bezahlvorgang verwendet werden. Gleiches gilt für beim Kauf von WM-Tickets gespeicherte Daten: Diese dürfen nur für die Abwicklung des Ticketkaufs verwendet werden. Zulässig wäre hingegen z.B. die Verarbeitung personenbezogener Daten für die Gepäckermittlung bei Flugreisen.

Für die Länge der Speicherung ergibt sich Folgendes: Die Speicherung ist für die Dauer der Durchführung des Vertrags zulässig. Ein Vertrag gilt als durchgeführt, wenn die Ware geliefert und die Gewährleistungsfrist beendet ist.¹³⁷ Nach geltendem Recht dürfte daher eine Speicherung von zwei Jahren nach § 28 Abs. 1 S. 1 Nr. 1 BDSG legitim sein, da die regelmäßige gesetzliche Gewährleistungsfrist zwei Jahre beträgt.¹³⁸ Welche Daten im Einzelnen verarbeitet werden dürfen, kann nicht abstrakt beurteilt werden, sondern richtet sich stets nach der jeweiligen konkreten Ausgestaltung des Vertragsverhältnisses.¹³⁹ Zulässig wird i.d.R. die Verarbeitung der sog. Stammdaten sein. Hierbei handelt es sich üblicherweise um den vollständigen Namen, die Anschrift und in einigen Fällen auch um weitere Angaben wie das Geburtsdatum, die Telefonnummer und die E-Mail-Adresse. Es muss im Einzelfall überprüft werden, welche Daten für die Vertragsabwicklung erforderlich sind.

¹³⁴ *Hoeren*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4.6, Rn. 17.

¹³⁵ *Simits*, in: Simits, Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 28 Rn. 79 m. w. N.

¹³⁶ *Hoeren*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4.6, Rn. 19.

¹³⁷ *Hoeren*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4.6, Rn. 21.

¹³⁸ § 438 Abs. 1 Nr. 3 BGB.

¹³⁹ *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 28 Rn. 18; *Simits*, in: Simits, Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 28 Rn. 82.

bb) Wahrnehmung berechtigter Interessen

Ferner kommt eine Speicherung personenbezogener Daten nach § 28 Abs. 1 S. 1 Nr. 2 BDSG in Betracht, soweit dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass ein überwiegendes schutzwürdiges Interesse des Betroffenen entgegensteht. Unter den Begriff des berechtigten Interesses fällt jedes tatsächliche, auch wirtschaftliche oder ideelle Interesse.¹⁴⁰ Ein berechtigtes Interesse kann daher jedes von der Rechtsordnung gebilligte Interesse sein.¹⁴¹ Die Verwendung der Daten muss zur Wahrung des berechtigten Interesses nicht nur dienlich, sondern erforderlich sein. Inwieweit die schutzwürdigen Interessen des Betroffenen vorrangig sind, kann nur im Rahmen einer Interessenabwägung ermittelt werden.¹⁴² Dabei ist zu beachten, dass sich aus der Wertentscheidung des § 4 BDSG ergibt, dass im Zweifel die Interessen des Betroffenen überwiegen.¹⁴³ Das Gesetz lehnt den Begriff der „schutzwürdigen Interessen“ entsprechend seinem Schutzziel nach § 1 BDSG an Begriffe wie „Privat-, Intim-, oder Vertraulichkeitssphäre“ an, die gleichzeitig Synonyme für das auf Art. 1, 2 GG beruhende „Recht auf informationelle Selbstbestimmung“ darstellen.¹⁴⁴

Sollen die bereits zulässigerweise zur Abwicklung des Vertragsverhältnisses erhobenen Daten beispielsweise zu Werbungs- und Marktforschungszwecken benutzt werden, so liegt eine Zweckänderung vor. Diese ist gem. § 28 Abs. 1 Nr. 2 BDSG nur dann zulässig, wenn die Datenerhebung zur Wahrung berechtigter Interessen des Unternehmens erforderlich ist. Die Durchführung von Werbemaßnahmen und Marktanalysen wird von der herrschenden Meinung als berechtigtes Interesse eines Unternehmens bewertet.¹⁴⁵ Für die Stammdaten wie Name und Anschrift lässt sich feststellen, dass teilweise kein schutzwürdiges Interesse des Betroffenen der Verwendung der Daten entgegensteht. So wird der Kunde i.d.R. davon ausgehen müssen, dass die z.B. im Rahmen eines Kundenkartenvertragsmodells einmal erhobenen Daten auch zu Werbezwecken verwendet werden.¹⁴⁶

In Kombination mit einem RFID-Chip können aber auch weitere Informationen erlangt werden, wenn ein Kunde ein Tag etwa in einem Supermarkt mit sich führt und darüber identifizierbar ist (z.B. durch ein Tag in einer Kundenkarte). Würden beispielsweise an Ein- und Ausgang Reader aufgestellt, so könnte festgehalten werden, wann ein bestimmter Kunde das jeweilige Geschäft betritt und wann er es verlässt. Die Erhebung dieser Daten würde der Bestimmung der Verweildauer des Kunden im Geschäft dienen, was keine Ausnahme von der Einwilligungspflicht gem. § 28 Abs. 1 Nr. 2 BDSG begründen würde, da ein schutzwürdiges Interesse des Unternehmens an dieser Information nicht ersichtlich ist.¹⁴⁷ Informationen über das Kaufverhalten eines Verbrauchers könnte das Unternehmen durch Lesegeräte erlangen, die in bestimmten Abteilungen platziert werden und so registrieren

140 VGH Mannheim, NJW 1984, 1912.

141 *Schaffland/Wiltfang*, Bundesdatenschutzgesetz-Kommentar, a. a. O., § 28 Rn. 85.

142 *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 28 Rn. 36.

143 *Hoeren*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4.6, Rn. 33.

144 *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 28 Rn. 35.

145 *Simitis*, in: Simitis Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 28 Rn. 137; *Schaffland/Wiltfang*, Bundesdatenschutzgesetz-Kommentar, a. a. O., § 28 Rn. 92.

146 Gutachten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), Kundenbindungssysteme und Datenschutz, a. a. O., S. 72.

147 Auch eine Ausnahme nach § 28 Abs. 1 S. 1 Nr. 1 BDSG läge nicht vor, da die erhobenen Daten weder der Abwicklung des potenziellen Kaufvertrags noch der Abwicklung des Bonus- Serviceprogramms dienen würden.

können, welche Bereiche des Geschäfts der Kunde bevorzugt aufsucht. Das Erstellen solcher umfassenden Bewegungsprofile begegnet durchgreifenden datenschutzrechtlichen Bedenken, da es sich hierbei um einen intensiven Eingriff in die Privatsphäre des Kunden handelt.¹⁴⁸ An der Erlangung derartiger Daten besteht wiederum kein schützenswertes Interesse des Unternehmers, so dass zur Erhebung dieser Informationen ebenfalls die Einwilligung des Kunden erforderlich ist.¹⁴⁹

cc) Allgemein zugängliche Quellen

Die Datenverarbeitung ist gem. § 28 Abs. 1 S. 1 Nr. 3 BDSG auch dann zulässig, wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, sofern nicht ein entgegenstehendes Interesse des Betroffenen offensichtlich überwiegt. Unter einer allgemein zugänglichen Quelle versteht man eine Informationsquelle, die technisch zur Eignung bestimmt ist, einem individuell nicht bestimmbar Personenkreis Informationen zu verschaffen.¹⁵⁰ Zu solchen Quellen zählen insbesondere öffentliche Register wie Schuldnerverzeichnisse, Handels- und Vereinsregister, Zeitungen, Adressbücher, Telefonbücher, Rundfunk und Internetseiten, sofern ohne zusätzliche Kenntnis bestimmter Umstände auf die Daten zugegriffen werden kann.¹⁵¹ Zudem ist zu prüfen, ob nicht ausnahmsweise das schutzwürdige Interesse des Betroffenen der Datenverarbeitung offensichtlich entgegensteht. Aus dem Begriff „offensichtlich“ ergibt sich, dass eine Speicherung der Daten im Zweifel zulässig sein soll. Die verarbeitende Stelle ist daher nicht zu einer intensiven Einzelfallprüfung verpflichtet, es sei denn das Gegeninteresse liegt klar auf der Hand.¹⁵²

f) Sondervorschriften für mobile Speichermedien

aa) Anwendungsbereich

Eine besondere Ausprägung des Transparenzgebots findet sich in § 6c Abs. 1 BDSG, wonach für den Unternehmer bei der Verwendung von mobilen personenbezogenen Speicher- und Verarbeitungsmedien besondere Unterrichtungspflichten bestehen.¹⁵³ Unter solchen Medien sind Datenträger zu verstehen, auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.¹⁵⁴ Betroffen sind hier also vor allem Anwendungen der dritten Fallgruppe, also solche, bei denen personenbezogene Daten direkt auf dem Tag gespeichert werden. Die besonderen Informationspflichten sind deshalb notwendig, da die Kontrolle bei diesen Medien aufgrund der Tatsache, dass keine Schnittstelle zwischen Mensch und Gerät besteht, dem Besitzer entzogen wird.¹⁵⁵

148 Das Erstellen von Persönlichkeitsprofilen, d.h. die langfristige Speicherung von Daten aus unterschiedlichen Lebensbereichen, ist unzulässig, da es gegen das Menschenbild des Grundgesetzes verstößt und somit verfassungswidrig ist; vgl. BVerfG, NJW 1969, 1707; BVerfG, NJW 1984, 424; allgemein zu dieser Thematik: Weichert, in: Kilian/Heussen, Computerrechts-Handbuch, Stand März 2005, S. 130 (Rn. 31 f.).

149 *Holznagel/Bonnekoh*, MMR 2006, 17, 20.

150 BVerfGE 33, 52, 65.

151 *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 28 Rn. 45; Hoeren, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4.6, Rn. 35.

152 *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 28 Rn. 44.

153 Diese 2001 in das BDSG aufgenommene Informationspflicht soll einen weiteren Schritt des neuen BDSG zu mehr Transparenz für den Betroffenen bewirken, vgl. *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 6c Rn. 6.

154 So die gesetzliche Legaldefinition, vgl. § 3 Abs. 10 BDSG.

155 *Lahner*, DuD 2004, 723, 724.

Typischer Anwendungsfall sind sog. „Chipkarten“¹⁵⁶, also z.B. ec-Karten, Krankenversicherungskarten, SIM-Karten für die Nutzung von Mobilfunkdiensten, elektronische Tickets und auch zahlreiche Varianten der Kundenkarte.¹⁵⁷ Ist also eine Kundenkarte mit einem RFID-Chip ausgestattet, auf dem personenbezogene Daten gespeichert sind, so ist der Anwendungsbereich des § 6c BDSG eröffnet.¹⁵⁸

Bei den Transpondern selbst ist eine differenzierte Betrachtung erforderlich, je nachdem, ob eine über die bloße Speicherung hinausgehende automatisierte Verarbeitung möglich ist. Dies ist zweifelsohne bei Funkchips im High-End-Bereich der Fall, die über einen Mikroprozessor und ein Betriebssystem verfügen und zum Teil auch mit zusätzlichen kryptografischen Koprozessoren ausgestattet sind.¹⁵⁹ Bei diesen Tags reicht die Kapazität zur Speicherung von personenbezogenen Daten aus. Der Verarbeitungsvorgang kann auf dem mobilen Medium selbst stattfinden.¹⁶⁰ Bei Transpondern im Low-End-Bereich bestehen weder Speichermöglichkeiten, noch sind Verarbeitungsschritte auf diesen Transpondern durchführbar. Bei RFID-Chips mit mittlerer Speicherkapazität muss im Einzelfall untersucht werden, ob eine über die Speicherung hinausgehende automatisierte Verarbeitung möglich ist. Bei einem einfachen ROM-Speicher werden die Daten z.B. dauerhaft und unveränderlich gespeichert. Sie können weder elektrisch noch optisch gelöscht oder verändert werden.¹⁶¹ Hier wäre der Anwendungsbereich des § 6c BDSG folglich nicht eröffnet.¹⁶² Solche Transponder finden sich z.B. im Bereich des Lagermanagements, wo ausschließlich Seriennummern zur Identifizierung der Ware gespeichert werden. Eine darüber hinausgehende automatisierte Verarbeitung der Daten findet nicht auf den Chips statt. Etwas anderes gilt aber beim Einsatz eines Read-write-Systems. Diese verfügen über einen beschreibbaren EEPROM¹⁶³-Speicher, der elektronisch programmier- und löschar ist¹⁶⁴ und bei dem auch einfache Verschlüsselungsverfahren implementiert werden können.¹⁶⁵

Werden RFID-Tags im Einzelhandel eingesetzt, so handelt es sich dabei in der Regel um passive Tags, d.h. um solche, die keine Daten verarbeiten.¹⁶⁶ Solche „dummen“ Speichermedien sind nach der Gesetzesbegründung ausdrücklich von der Regelung nicht erfasst.¹⁶⁷ Ein Medium, das lediglich ein automatisiertes Auslesen von Informationen aus dem Medium ermöglicht, erfüllt daher nicht die Voraussetzungen von § 3 Abs. 10 Nr. 2 BDSG.¹⁶⁸ Eine Unterrichtungspflicht nach § 6c BDSG besteht bei Transpondern, auf denen ausschließlich ein EPC gespeichert wird, auch deshalb nicht, weil auf den Tags keine personenbezogenen Daten gespeichert sind.

156 Siehe hierzu ausführlich *Weichert*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 9.5; *ders.*, DuD 1997, 266 ff.

157 *Bizer*, in: Simitis, Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 6c Rn. 6 f.

158 So auch *Gräfin von Westerholt/Döring*, CR 2004, 710, 714.

159 *Lahner*, DuD 2004, 723, 724; zu den Speicherkapazitäten im Einzelnen siehe unter II. 5.

160 *Lahner*, DuD 2004, 723, 724.

161 BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 30.

162 A. A. *Lahner*, der den Anwendungsbereich des § 6c BDSG auch auf diese Arten von Transpondern ausdehnen will, vgl.

Lahner, DuD 2004, 723, 725 f.

163 Vgl. o. Fn. 33.

164 *Lahner*, Datenschutzrechtliche Probleme beim Einsatz von RFID-Systemen, a. a. O., S. 10 m. w. N.

165 *Finkenzeller*, RFID-Handbuch, a. a. O., S.25.

166 Vgl. oben unter II. 2.

167 BT-Drucks. 14/5793, S. 60.

168 *Bizer*, in: Simitis, Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 3 Rn. 277.

bb) Unterrichtungspflichten

Wird ein mobiles Speicher- und Verarbeitungsmedium eingesetzt, muss der Unternehmer dem Kunden seine Identität und Anschrift mitteilen (Nr. 1) und ihn über die Funktionsweise des Mediums aufklären, wobei hier keine detaillierte technische Beschreibung erfolgen soll, sondern für den Laien verständliche Informationen zu erteilen sind.¹⁶⁹ Außerdem muss der Betroffene wissen, wie er seine Rechte auf Auskunft und Korrektur nach den §§ 19, 20, 34 und 35 BDSG im Hinblick auf die Besonderheiten des Mediums ausüben kann (Nr. 3).

g) Verstoß gegen datenschutzrechtliche Vorschriften

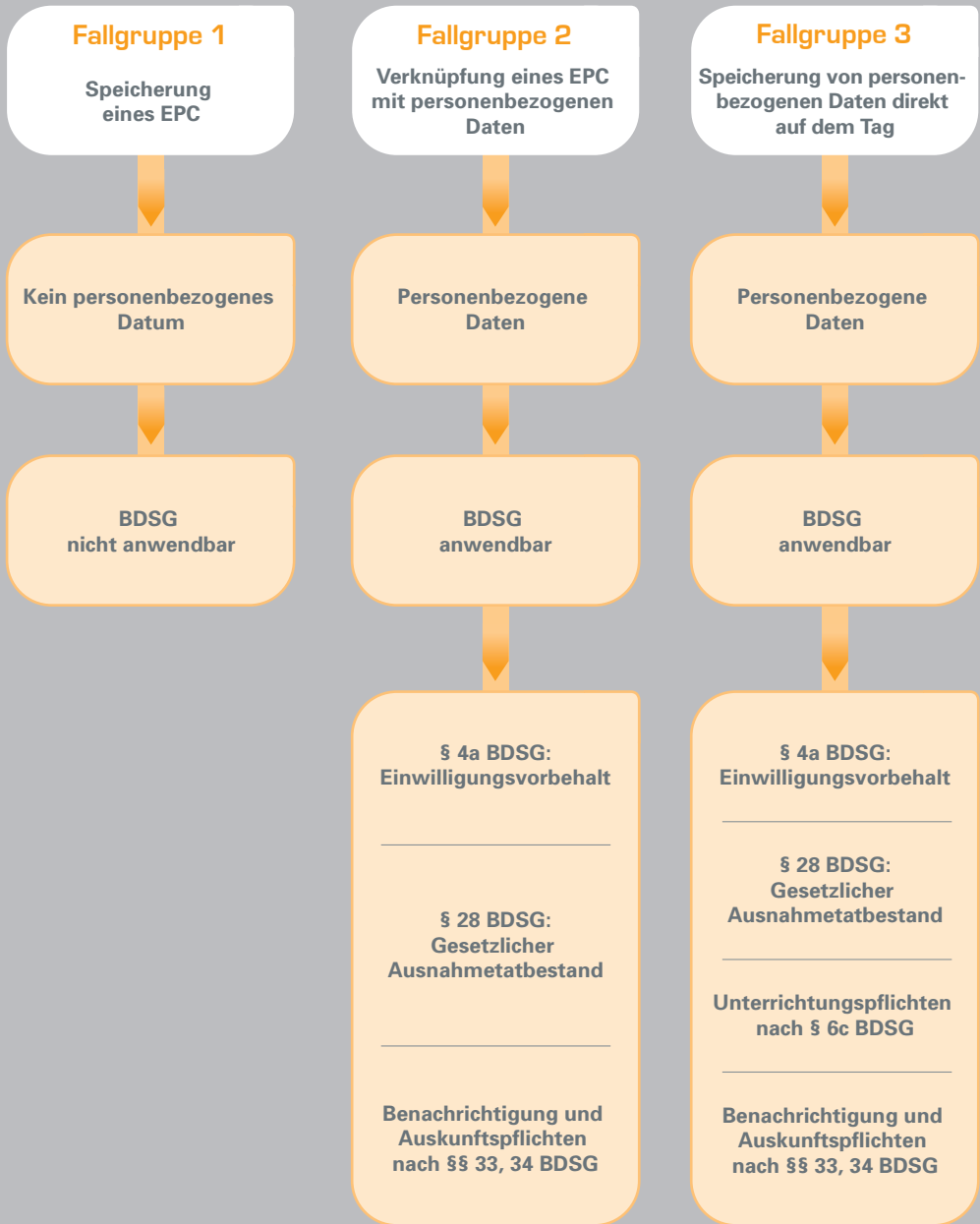
Der Verstoß gegen datenschutzrechtliche Vorschriften ist bußgeld- und ggf. strafbewehrt. Nach § 43 Abs. 2 Nr. 1 BDSG handelt ordnungswidrig, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet. Voraussetzung ist folglich, dass es sich um personenbezogene Daten handelt.¹⁷⁰ Eine solche Ordnungswidrigkeit kann mit einer Geldbuße von bis zu 250.000 € geahndet werden. Fahrlässiges Handeln kann allerdings nur mit der Hälfte des jeweils angedrohten Höchstbetrages belegt werden, § 17 Abs. 2 OWiG. Nach § 44 Abs. 1 StGB ist eine Handlung nach § 43 Abs. 2 Nr. 1 BDSG sogar strafbar, wenn sie gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begangen wird. Die Tat kann mit Freiheitsstrafe von bis zu zwei Jahren oder mit Geldstrafe bestraft werden.

h) Fazit

Als Zwischenergebnis kann festgehalten werden, dass personenbezogene Daten auch bei der Verwendung der Transpondertechnologie durch die geltenden Bestimmungen des BDSG geschützt sind. Personenbezogene Daten sind tangiert und damit der Anwendungsbereich des BDSG eröffnet, wenn Angaben über persönliche oder sachliche Verhältnisse einer Person unmittelbar auf dem Tag gespeichert werden. Des Weiteren ist dies der Fall, wenn eine Verknüpfung über das Tag mit solchen Daten möglich ist, die in einer Datenbank gespeichert sind. Ist das BDSG anwendbar, so ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach § 4 Abs. 1 BDSG nur dann zulässig, wenn der Betroffene eingewilligt hat oder das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet. Auch die weiteren datenschutzrechtlichen Grundsätze wie das Prinzip der Erforderlichkeit, der Transparenz- und der Zweckbindungsgrundsatz sind zu beachten. Werden mobile Speichermedien eingesetzt, bestehen zusätzliche Unterrichtungspflichten des Verwenders. Bei einem elektronischen Produktcode, der auf einem RFID-Tag gespeichert ist, handelt es sich nicht um ein personenbezogenes Datum, so dass datenschutzrechtliche Vorschriften nicht anwendbar sind.

¹⁶⁹ *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 6c Rn. 6.

¹⁷⁰ Zu der Frage, wann es sich bei Daten, die auf RFID-Tags gespeichert sind, um personenbezogene Daten handelt, s. ausführlich unter IV. 1. a).



2. RECHT DER DATENSICHERHEIT

Neben den Chancen, die die RFID-Technologie für die Gesellschaft und Wirtschaft eröffnet, entstehen auch neue Risiken. Der wirtschaftliche Erfolg wird nicht zuletzt auch davon abhängen, inwieweit es gelingt, die anfallenden Daten gegen Datenverlust und -missbrauch zu schützen.¹⁷¹ Im folgenden Abschnitt wird daher erörtert, welche Gefahren für RFID-Anwendungen bestehen (dazu unter a)), welche technischen Lösungswege bestehen (dazu unter b)) und welche rechtlichen Verpflichtungen zum Ergreifen von Sicherheitsmaßnahmen existieren (dazu unter c)). Anschließend wird der strafrechtliche Schutz erläutert (dazu unter d)).

a) Gefahren für die Datensicherheit

Als Erstes soll untersucht werden, welchen technischen Sicherheitsrisiken die RFID-Technologie ausgesetzt ist. Bei der Speicherung von Daten auf einem Tag kann sich in mehrfacher Hinsicht eine spezifische Bedrohungslage ergeben.¹⁷² Bedrohungen können sich ergeben für die Verfügbarkeit von Daten, deren Integrität, Vertraulichkeit und Authentizität.¹⁷³

aa) Abhören der Kommunikation

Eine der signifikanten Bedrohungslagen für RFID-Systeme besteht im Abhören der Kommunikation zwischen Transponder und Lesegerät. Dabei wird die Kommunikation über die Luftschnittstelle durch Auffangen und Dekodieren der Funksignale abgehört.¹⁷⁴ Die Kommunikation handelsüblicher Tags läuft größtenteils im 125-kHz- oder im 13,56-MHz-Bereich ab. Wird nun eine im ISO-Standard 14443 definierte Funkschnittstelle verwendet, so liegt diese im Kurzwellenband und kann mit handelsüblichen Breitband- oder Weltempfängern empfangen werden.¹⁷⁵ Auch die Reichweite von RFID-Systemen hat Auswirkungen auf die Abhörmöglichkeit. Die aktive Kommunikation kann nur aus Abständen von 10 bis 15 cm (ISO 14443) oder maximal 1,5 m (ISO 15693) als typische Arbeitsabstände abgehört werden. Das passive Abhören ist jedoch auch aus größeren Abständen möglich. Ein Experiment ergab, dass ein passives Abhören der Kommunikation von RFID-Systemen nach ISO 14443 bis zu mehreren Metern und damit weit über den spezifischen Arbeitsbereich von 10–15 cm hinaus möglich ist.¹⁷⁶

Die praktischen Konsequenzen, die sich hieraus ergeben, stellen ein Risiko sowohl für den Verwender von RFID als auch für den Verbraucher dar, der beispielsweise Produkte bei sich trägt, die durch RFID-Chips gekennzeichnet sind. Für den Verwender besteht die Gefahr der Industriespionage. Konkurrenten oder Wirtschaftsspione könnten die auf den Tags gespeicherten Daten ausspähen, um

171 BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 101.

172 Zu den unterschiedlichen Bedrohungslagen umfassend Kapitel 7 der BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., wobei hier die verschiedenen Angriffsarten auch nach den unterschiedlichen Bedrohungslagen der aktiven (Betreiber der RFID-Systeme) und der passiven Partei (insbesondere Kunden und Arbeitnehmer) differenziert werden.

173 *Holzner*, Recht der IT-Sicherheit, 2003, S. 12 ff.

174 BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 42.

175 *Finke/Kelter*: Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO 14443-Systems.

176 *Finke/Kelter*: Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO 14443-Systems.

sich so einen Wettbewerbsvorteil zu verschaffen. Kunden oder auch Arbeitnehmer, die Tags oder mit Tags gekennzeichnete Objekte benutzen, tragen ein anderes Risiko. Sie haben keine Kontrolle über die Daten, die auf den Tags gespeichert sind. Auf RFID-Chips gespeicherte Daten könnten durch einzelne Kriminelle unbefugt ausgelesen werden. Theoretisch könnte dadurch das Konsumverhalten von Kunden ausgeforscht werden, wenn die jeweilige Person bestimmbar ist. Dient ein RFID-Chip der Zutrittskontrolle, so ist es rein technisch betrachtet auch möglich, dass Arbeitnehmer auf ihre Anwesenheit und Leistung hin kontrolliert werden.

Denkbar ist auch, dass Datenspuren, die bei der Verwendung von RFID anfallen, zu Strafverfolgungszwecken gebraucht werden. So wie derzeit die Telekommunikationsüberwachung bei Vorliegen des Verdachts einer bestimmten Straftat gem. § 100a StPO möglich ist, könnten staatliche Überwachungsmaßnahmen auf das „Internet der Dinge“ ausgeweitet werden.¹⁷⁷

bb) Fälschung des Inhalts oder der Identität

Eine weitere Angriffsart besteht in der Fälschung des Inhalts oder der Identität eines Transponders.¹⁷⁸ Die Fälschung kann in mehreren Hinsichten erfolgen: Im ersten Fall werden die auf dem Tag gespeicherten Daten durch einen unautorisierten Schreibzugriff verändert. Die Seriennummer bleibt dabei unverändert, so dass das Lesegerät die Identität des Transponders weiterhin korrekt erkennt. Im zweiten Fall bringt sich der Angreifer dagegen in den Besitz der Seriennummer und eventuell darüber hinausgehender Sicherheitsinformationen eines Tags und missbraucht diese zur Vortäuschung der entsprechenden Identität. Er könnte den RFID-Chip klonen, wodurch dann mehrere Tags der scheinbar gleichen Identität in Umlauf gelangen könnten. Mithilfe der abgehörten Kommunikationsinhalte kann ein Angreifer das jeweilige Tag nachbilden, indem er die Informationen im einfachsten Fall auf ein unbeschriebenes Tag aufbringt.¹⁷⁹ Drittens könnte ein Tag physisch vom Trägerobjekt getrennt und mit einem anderen Objekt verbunden werden. Dies entspricht von der strafrechtlichen Einordnung her dem „Umkleben“ von Preisschildern auf Waren.¹⁸⁰ Beim Ablösen des Tags vom Trägerobjekt können ferner dessen Bewegungen vor dem Lesegerät verborgen werden. Schließlich kann ein Angreifer auch die Identität eines autorisierten Lesegeräts vortäuschen, um die Daten eines Tags mit seinem eigenen Lesegerät auslesen zu können.

¹⁷⁷ So ein fiktives Fallbeispiel der BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 102.

¹⁷⁸ BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 42.

¹⁷⁹ Kelter/Wittman, DuD 2004, 331, 333.

¹⁸⁰ Zur strafrechtlichen Bewertung des Umklebens von Preisetiketten vgl. z.B. Tröndle, in: Leipziger Kommentar, § 267 Rn. 147 f.

cc) Störung des Datenaustauschs

Die Sicherheit von RFID-Systemen kann auch durch das Stören des Datenaustauschs durch Denial-of-Service-Angriffe (DoS-Angriffe) beeinträchtigt werden. Der Datenaustausch kann zum einen aktiv, z.B. durch Benutzen eines Störsenders, behindert werden. Wenn dieser Störsender ein ausreichendes künstliches Umgebungsrauschen erzeugt, sind Tag und Reader nicht mehr in der Lage, dieses Signal durch ihr eigenes Nutzsignal zu überlagern.¹⁸¹ Außerdem kann der Datentransfer durch den unautorisierten Gebrauch von Deaktivierungsbefehlen unterbrochen werden.

Die Störung des Datenaustauschs kann zum anderen auch passiv erfolgen. Ein passiver DoS-Angriff ist durch Abschirmen möglich. Dabei wird ein Tag so mit einer schirmenden Hülle versehen, dass ein Radio-Frequency-Feld diese Schirmung nicht mehr durchdringen kann. Dies würde allerdings voraussetzen, dass der Besitzer des Transponders sein Tag absichtlich abschirmt. Die Gefahr ist hier daher eher als gering einzustufen, zumal nur ein einzelnes Tag betroffen wäre und alle anderen im Ansprechbereich befindlichen RFID-Transponder nicht beeinflusst würden.¹⁸² Relevanter für die Sicherheit von RFID-Systemen ist hingegen der Einsatz sog. „Blocker-Tags“. Durch Blocker-Tags kann gegenüber dem Lesegerät eine beliebig große Anzahl von anwesenden Transpondern vorgetäuscht werden, so dass das Lesegerät eine entsprechend große Anzahl von vergeblichen Tag-Anforderungen abarbeiten muss und dadurch blockiert wird.¹⁸³ Blocker-Tags wurden ursprünglich aus Gründen des Verbraucherschutzes entwickelt. Es liegt jedoch nahe, dass diese Tags bewusst oder unbewusst auch zu Störungen sinnvoller RFID-Anwendungen führen können.

Eine weitere Gefahr besteht im Zerstören der RFID-Chips. Transponder können durch physische Gewalteinwirkung oder auch durch Mikrowellenstrahlung beschädigt oder zerstört werden.¹⁸⁴ Das gleiche Ergebnis kann auch durch die Verwendung von elektromagnetischen Feldern erreicht werden. Ein passives Tag bezieht seine Energie aus dem magnetischen Feld des Lesegeräts. Wird nun ein geeignetes Feld erzeugt, das hinreichend stark ist, so kann die Kopplungseinheit des Tags oder sogar das gesamte Tag zerstört werden.¹⁸⁵

181 *Kelter/Wittman*, DuD 2004, 331, 333.

182 *Kelter/Wittman*, DuD 2004, 331, 333.

183 BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 42.

184 *Kelter/Wittman*, DuD 2004, 331, 333.

185 *Kelter/Wittman*, DuD 2004, 331, 333.

dd) Angriff auf das Backend

Schließlich können sich Angriffe auf das Backend¹⁸⁶ von RFID-Systemen beziehen. Auch hier besteht das Risiko des Abhörens. Ist das Backend mit dem Internet verbunden, so ergeben sich zusätzliche Gefahren durch Hacking und durch das Einbringen von Software-Anomalien wie Viren und Würmer. Dadurch kann auch die Identität eines Lesegeräts mit autorisiertem Zugang zum Backend gefälscht werden.¹⁸⁷ Allerdings handelt es sich hierbei nicht um RFID-spezifische, sondern um allgemeine IT-Sicherheitsrisiken, die mit den üblichen IT-Sicherheitsverfahren abgewehrt werden können. Diese lassen sich leichter neuen Erfordernissen anpassen als Sicherheitsverfahren, die auf den Tags implementiert werden.

b) Technische Sicherheitsmaßnahmen

Ausgehend von den oben geschilderten Angriffsmöglichkeiten bieten sich folgende Sicherheitsmaßnahmen an:

aa) Authentifizierung

Authentizität ist gewährleistet, wenn durch geeignete Kontrollmaßnahmen sichergestellt wird, dass Daten und Informationen wirklich aus der angegebenen Quelle stammen bzw. dass die Identität des angeschlossenen Systems korrekt ist.¹⁸⁸ Um das Abhören der Kommunikation und die Fälschung von Transpondern zu verhindern, können Authentifizierungsmechanismen in RFID-Systeme implementiert werden. Zur Überprüfung der Identität eines Lesegeräts kann z.B. ein Passwortschutz eingerichtet werden. Dabei identifiziert sich das Lesegerät gegenüber dem Tag durch Übertragung eines Passworts, das der Transponder mit dem gespeicherten Passwort vergleicht, und gestattet den Zugriff auf die gespeicherten Daten nur, wenn beide miteinander übereinstimmen.¹⁸⁹

Auch die Identität des Tags ließe sich überprüfen. Die Gefahr der Identitätsfälschung wird häufig von Verbraucher- und Datenschutzorganisationen moniert. Eine Möglichkeit zur Erhöhung der Sicherheit könnte in der weltweit eindeutigen Regelung zur Vergabe der Seriennummern von Tags bestehen, wie es z.B. bei der Nutzung des elektronischen Produktcodes (EPC) bereits der Fall ist.¹⁹⁰ Hier wäre eine weltweite Standardisierung erforderlich, wie sie durch EPCglobal für den Bereich Handel und Konsumgüterindustrie entwickelt wird. Die im Jahre 2003 gegründete Non-profit-Organisation entwickelt wirtschaftliche und technische Standards für den elektronischen Produktcode. Ziel ist es, ein Netzwerk aufzubauen und die Verbreitung standardisierter Prozesse voranzutreiben. Diese Vorgehensweise würde zumindest einen gewissen Schutz vor gefälschten Tags bieten. Jedenfalls könnte dadurch das Auftreten nicht vergebener Nummern oder von geklonten Tags erkannt werden.

¹⁸⁶ Unter Backend versteht man die Datenbestände, mit denen die vom Lesegerät erfassten Daten über weitere Kommunikationskanäle verknüpft werden, vgl. oben unter II. 5.

¹⁸⁷ BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 44.

¹⁸⁸ Holznaegel, Recht der IT-Sicherheit, a. a. O., S. 14 Rn. 9.

¹⁸⁹ BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 48.

¹⁹⁰ BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 47.

Die Authentifizierung des Tags könnte auch durch ein Challenge-Response-Verfahren sichergestellt werden.¹⁹¹ Dabei sendet das Lesegerät an das Tag eine Zufallszahl oder einen Zeitstempel (Challenge), die dieses dann verschlüsselt an das Lesegerät zurücksendet (Response). Der Schlüssel beweist dem Lesegerät die Identität des Tags und wird nie mitübertragen. Das Challenge-Response-Verfahren setzt jedoch eine gewisse Speicherkapazität des verwendeten Tags voraus, da es Zufallszahlen generieren können muss.

bb) Verschlüsselung

Eine höhere Sicherheit gegen das Auslesen von Daten wird durch eine Verschlüsselung der Daten mittels des Hash-Lock-Verfahrens erreicht.¹⁹² Vor dem erstmaligen Beschreiben eines Tags wird mithilfe einer Hash-Funktion aus einem Schlüssel eine sog. Meta-ID als Pseudonym für das Tag erzeugt und im Tag gespeichert, wodurch das Tag gesperrt wird („locked“). Auf die Signale eines Lesegeräts reagiert es dann nur noch mit dem Senden der Meta-ID. Erst wenn das Lesegerät in einer Backend-Datenbank den zur Meta-ID gehörenden Schlüssel abgerufen und zum Tag übertragen hat, wird dieses entsperrt, falls das Ergebnis der auf den Schlüssel angewandten Hash-Funktion mit der Meta-ID identisch ist.¹⁹³ In diesem Fall ist das Lesegerät authentifiziert und gibt den Zugriff auf seine Daten frei. Auch beim Einsatz kryptografischer Verfahren müssen die Tags eine gewisse Speicherkapazität aufweisen.

cc) Verhinderung des Auslesens durch Blocker-Tags

Das unautorisierte Auslesen von auf Transpondern gespeicherten Daten kann durch den Einsatz sog. Blocker-Tags verhindert werden. Ein Blocker-Tag ist ein Transponder, der sämtliche Anfragen eines Lesegeräts positiv beantwortet und dieses dadurch derart verwirrt, dass das eindeutige Identifizieren eines bestimmten Tags unmöglich gemacht wird.¹⁹⁴ Ein Kunde könnte ein solches Blocker-Tag in seinem Einkaufsbeutel mit sich führen und so verhindern, dass die von ihm gekauften Produkte von Dritten erkannt werden können.

Unerwünschter Nebeneffekt kann jedoch die ungewollte Störung anderer RFID-Anwendungen in der Umgebung sein. Es ist daher geplant, Blocker-Tags auf bestimmte Seriennummernbereiche zu begrenzen und somit nur Labels bestimmter Nummernbereiche auszuschalten.¹⁹⁵ Dies hätte zur Folge, dass beispielsweise die RFID-Warenwirtschaft innerhalb eines Supermarkts nicht gestört würde. Beim Bezahlen an der Kasse könnten die Labels dann umkodiert werden und dadurch in den Blockadebereich der Störsender fallen. Der Verbraucher könnte dann autonom darüber entscheiden, ob er seine möglicherweise unbewusst mitgeführten Tags durch ein Blocker-Tag maskiert oder ob er darauf verzichtet.

191 BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 47.

192 Hierzu BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, a. a. O., S. 48 f.

193 Weis, Security and Privacy in Radio-Frequency Identification Devices, 2003, S. 38 f.; Weis/Sarma/Rivest/Engels, Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, 2003, S. 7.

194 S. dazu bereits oben unter IV. 2. a) cc).

195 Kelter/Wittman, DuD 2004, 331, 334.

dd) Deaktivierung durch Kill-Befehl

Um auf Konsumgütern angebrachte Tags zu deaktivieren, kann durch einen sog. Kill-Befehl die Seriennummer derart anonymisiert werden, dass diese nicht mehr ausgelesen werden kann. Dieses Vorgehen bringt jedoch einige Nachteile mit sich. Kritisiert wird zum einen, dass derzeit nur die Deaktivierung eines einzelnen Transponders möglich ist, so dass jedes gekaufte Produkt einzeln behandelt werden muss. Es werden jedoch bereits Technologien entwickelt, die diesen Vorgang vereinfachen.¹⁹⁶ Unpraktikabel ist der Einsatz des Kill-Befehls teilweise auch vor dem Hintergrund, dass der Kunde den Vorgang der Deaktivierung nicht überprüfen kann. Dem lässt sich jedoch abhelfen, indem ein Lesegerät zur Verfügung gestellt wird, mit dem Kunden, die dies wünschen, das jeweilige Tag selbst auslesen und so die Deaktivierung kontrollieren können. Ein Nachteil der permanenten Deaktivierung liegt darin, dass die positiven Nutzungsmöglichkeiten, wie die Verwendung von Daten bei Umtausch, Reparatur, Weiterverkauf oder Recycling, verloren gehen. Eine Lösung hierfür könnte eine neue Generation von Tags sein, bei denen der Kunde bei Bedarf die Verbindung zwischen Chip und Antenne durch einfaches Abreißen trennen und so die Aussendung von Funksignalen unterbinden kann. Dies hat den Vorteil, dass die gespeicherten Daten im Bedarfsfall aus sehr geringer Entfernung wieder gelesen werden können, sofern sie noch einmal benötigt werden.¹⁹⁷

c) Rechtliche Verpflichtungen zur Sicherung personenbezogener Daten

Im Folgenden sollen die rechtlichen Verpflichtungen zum Ergreifen von Datensicherungsmaßnahmen in Bezug auf personenbezogene Daten dargestellt werden. Datensicherung umfasst alle technischen und organisatorischen Maßnahmen, die zur Sicherstellung der Datensicherheit getroffen werden.¹⁹⁸

aa) Anforderungen des BDSG

Das BDSG schreibt Maßnahmen zur Datensicherung und Datenschutzkontrolle in verschiedenen Bestimmungen vor, auch wenn die Begriffe hierbei nicht ausdrücklich genannt werden. Die verantwortlichen Stellen werden teilweise zu konkreten personellen (§§ 4f, 4g Abs. 1 BDSG), organisatorischen (§ 5 BDSG) oder technischen Maßnahmen verpflichtet. Zentrale und entscheidende Norm ist in diesem Zusammenhang jedoch § 9 BDSG.¹⁹⁹ Sowohl öffentliche als auch nicht-öffentliche Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, haben gem. § 9 S. 1 BDSG die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung des BDSG, insbesondere die in der Anlage zu § 9 BDSG genannten Anforderungen, zu gewährleisten. Auf RFID-Chips gespeicherte personenbezogene Daten sind daher durch geeignete technische und organisatorische Maßnahmen vor unbefugten Zugriffen zu sichern.

Nach § 9 S. 2 BDSG sind aber nur solche Maßnahmen erforderlich, deren Aufwand in einem ange-

¹⁹⁶ So auch *Langheinrich*, Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie, 2004, S. 14.

¹⁹⁷ Vgl. heise online, Meldung vom 10.3.2006, abrufbar unter <<http://www.heise.de/newsticker/meldung/70646>>.

¹⁹⁸ *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4.5, Rn. 1, vgl. auch *Ernestus/Geiger*, in: Simitis Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 9 Rn. 2 f.; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, a. a. O., S. 384.

¹⁹⁹ *GolalSchomerus*, BDSG-Kommentar, a. a. O., § 9 Rn. 4.

messenen Verhältnis zum Schutzzweck steht. Diese Einschränkung stellt klar, dass nur solche Maßnahmen gefordert werden können, die dem im Grundgesetz verankerten Verhältnismäßigkeitsgrundsatz entsprechen. Die Abwägung zwischen Aufwand und Schutzzweck der Norm führt allerdings nicht selten zu dem Ergebnis, dass höchster Aufwand gerechtfertigt ist, um die Schutzziele zu erreichen.²⁰⁰ Die Verhältnismäßigkeit ist die einzige Auswahlrichtlinie, die das BDSG den Daten verarbeitenden Stellen vorgibt. Es ist aber mittlerweile anerkannt, dass die Gesamtheit der Maßnahmen zum technischen Datenschutz in einem Verfahren oder bei einer Daten verarbeitenden Stelle auf der Grundlage eines Sicherheitskonzepts zusammengestellt werden muss.²⁰¹ Dieses muss sich dem Stand der Technik entsprechend angemessen gegen realistische Bedrohungen richten. Als anerkannte Methoden zur Entwicklung solcher Sicherheitskonzepte sind das IT-Sicherheitshandbuch und das jährlich aktualisierte IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnologie (BSI) zu nennen.²⁰²

bb) Die Anlage zu § 9 BDSG

In der Anlage zu § 9 BDSG ist geregelt, dass bei automatisierter Datenverarbeitung die innerbetriebliche bzw. innerbetriebliche Organisation so zu gestalten ist, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Relevant ist hier insbesondere die in Punkt 3 geregelte Zugriffskontrolle und die in Punkt 4 niedergelegte Weitergabekontrolle. Die Zugriffskontrolle schreibt Maßnahmen vor, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Regelung betrifft also primär die Begrenzung des Zugriffs für die zur Benutzung eines Datenverarbeitungssystems an sich Berechtigten auf die Daten, die im Rahmen der jeweiligen Zugriffsberechtigung liegen.²⁰³ Zugriff ist der Zugang zu den personenbezogenen Daten zum Zwecke ihrer Verwendung. Umfasst ist daher jede Aktivität in Bezug auf die gespeicherten Daten, die den Informationswert verfügbar macht, insbesondere die Kenntnisnahme oder die Nutzung der Daten.²⁰⁴ Die Zugriffsberechtigung ist die Befugnis, mit einer bestimmten Menge von Daten in einer definierten Weise umzugehen. Diese Befugnis der einzelnen Mitarbeiter ist von der verantwortlichen Stelle datenschutzgerecht zu bestimmen.

200 *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4.5, Rn. 26.

201 *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4.5, Rn. 30. Das nordrhein-westfälische Landesdatenschutzgesetz hat diesen Aspekt konsequent in § 10 Abs. 3 DSG NW umgesetzt. Nach dieser Vorschrift sind die zu treffenden technisch-organisatorischen Maßnahmen zu einem Sicherheitskonzept zusammenzuführen, welches auf einer Vorabkontrolle hinsichtlich möglicher Gefahren oder auf einer Risikoanalyse beruht.

202 Sowohl das IT-Sicherheitshandbuch als auch das IT-Grundschutzhandbuch sind über die Homepage des BSI abrufbar, <http://www.bsi.de/literat/sichhandbuch/sichhandbuch.zip>; <http://www.bsi.de/gshb/deutsch/index.htm>.

203 *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4.5, Rn. 45; Ernestus/Geiger, in: Simitis Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 9 Rn. 100.

204 *Ernestus/Geiger*, in: Simitis Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 9 Rn. 103.

In Punkt 4 ist geregelt, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf dem Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden dürfen. Die Daten sind also während der Übertragung besonders gegen den unbefugten Zugriff Dritter zu schützen. Dahinter verbirgt sich der Gedanke, dass Daten während dieser Phase der Verarbeitung besonders durch Angriffe von außen gefährdet sind. Als geeignete Maßnahme kann vor allem die Verschlüsselung der Daten vor der Übertragung angesehen werden.²⁰⁵ Daten sind aber auch besonders zu schützen, wenn sie auf einem Datenträger gespeichert sind.

cc) Bedeutung für RFID-Systeme

Insbesondere im Bereich der Datenverarbeitung im Backend sind Maßnahmen für eine ausreichende Zugriffskontrolle zu ergreifen (§ 9 BDSG i.V.m. Punkt 3 der Anlage zu § 9 S. 1 BDSG). Hier kommen insbesondere in Betracht:²⁰⁶

- ▶ Festlegen der Zugriffsbefugnisse der einzelnen Mitarbeiter
- ▶ Identifikation der Zugreifenden
- ▶ Protokollieren von Zugriffen und Missbrauchsversuchen
- ▶ Authentifizierung durch Passwort-Schutz
- ▶ Automatisches log-off nach einem bestimmten Zeitraum/nach Dienstschluss.

Auch in Bezug auf die Weitergabekontrolle sind erforderliche Maßnahmen zum Schutz der personenbezogenen Daten zu treffen. Werden personenbezogene Daten im Rahmen von RFID-Systemen übertragen, müssen diese gem. § 9 BDSG i.V.m. Punkt 4 der Anlage zu § 9 S. 1 BDSG grundsätzlich verschlüsselt²⁰⁷ werden. Außerdem können Maßnahmen zur Authentifizierung²⁰⁸ von Tag und Reader getroffen werden.

Hierbei ist aber insgesamt der Verhältnismäßigkeitsgrundsatz zu beachten. Es ist daher eine Abwägung zwischen dem Schutzbedürfnis und dem jeweils entstehenden Aufwand vorzunehmen. Als Aufwand sind sämtliche Kosten zu berücksichtigen, die von der Planungsphase bis zur Einführung entstehen, sowie die anfallenden Betriebskosten. Dazu zählen auch Entwicklungskosten und Investitionskosten, die in die eigentliche Sicherungstechnik fließen.²⁰⁹ Auf der anderen Seite ist zu bedenken, wie sensitiv die anfallenden Daten sind und wie hoch das Risiko für die Sicherheit dieser Daten ist. Insofern ist also möglichst eine Risikoanalyse durchzuführen. So ist z.B. für biometrische Daten in Ausweispapieren ein besonders hoher Schutz zu fordern, da es sich hier z. T. um besondere personenbezogene Daten (§ 3 Abs. 9 BDSG) handelt. In diesem Fall ist auch ein kostenintensiver Aufwand in Kauf zu nehmen. Andererseits kann für Transponder aus dem Low-End-Bereich beispielsweise kein kompliziertes kryptografisches Verfahren verlangt werden.

205 *Ernestus/Geiger*, in: Simitis Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 9 Rn. 112.

206 S. hierzu ausführlich *Ernestus/Geiger*, in: Simitis Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 9 Rn. 108 f.

207 Zur Verschlüsselung bereits näher unter IV. 2. b) bb).

208 Zu möglichen Authentifizierungsmaßnahmen bereits näher unter IV. 2. b) aa).

209 *Ernestus/Geiger*, in: Simitis Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 9 Rn. 34.

d) Strafrechtlicher Schutz

Die Sicherheit von RFID-Systemen wird auch durch Straftatbestände geschützt.

aa) Datenveränderung, § 303a StGB

Bei Angriffen auf RFID-Systeme kommt zunächst eine Strafbarkeit gem. § 303a StGB in Betracht. Danach macht sich strafbar, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Die Vorschrift schützt das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit der gespeicherten Daten.²¹⁰ Die unversehrte Verwendbarkeit wird durch die Authentizität und Integrität (Tatbestandsalternativen löschen, unbrauchbar machen und verändern) und durch die Verfügbarkeit (unterdrücken) der Daten sichergestellt. Der Datenbegriff des § 303a StGB ist identisch mit dem Datenbegriff des § 202a StGB. Anders als § 202a Abs. 1 StGB verlangt § 303a StGB aber nicht, dass die Daten nicht für den Täter bestimmt sind.²¹¹ Ebenso wie § 202a StGB schützt die Vorschrift diese Daten unabhängig von ihrem Inhalt.²¹² Nicht erforderlich ist, dass sie einen wirtschaftlichen, wissenschaftlichen, ideellen oder sonstigen Wert besitzen.²¹³

§ 303a StGB schützt Daten davor, gelöscht, unterdrückt, unbrauchbar gemacht oder verändert zu werden. Gelöscht werden Daten, wenn sie vollständig und unwiederbringlich unkenntlich gemacht werden.²¹⁴ Unterdrückt werden Daten, wenn sie dem Zugriff des Verfügungsberechtigten entzogen werden und deshalb von diesem nicht mehr verwendet werden können.²¹⁵ Dies wäre z.B. bei einer DoS-Attacke auf ein RFID-System der Fall. Daten sind dann unbrauchbar, wenn die bestimmungsgemäße Verwendbarkeit des Datenmaterials anders als durch Datenlöschung oder Datenunterdrückung aufgehoben wird.²¹⁶ Verändern umfasst diejenigen inhaltlichen Modifikationen einzelner Daten oder Abänderungen einer Datenfolge, die die Verwendbarkeit der Daten nicht aufheben, sondern nur beeinträchtigen oder zumindest modifizieren.²¹⁷

210 BT-Drs. 10/5058, 34.

211 Streng genommen erfasst der Tatbestand des § 303a StGB deshalb auch die Veränderung eigener Daten. Um dieses widersinnige Ergebnis zu vermeiden (die Vorschrift soll den Berechtigten vor unbefugter Veränderung durch Fremde schützen und nicht die Überarbeitung eigener Dateien verbieten), ist der Tatbestand auf das Verbot der Veränderung solcher Daten zu reduzieren, an deren Unversehrtheit ein anderer ein unmittelbares Interesse besitzt. Vgl. hierzu *Lenckner/Winkelbauer*, CR 1986, 824, 829.

212 *Möhrenschlager*, wistra 1986, 128, 141.

213 *Kühl*, in: Lackner/Kühl, StGB-Kommentar, 25. Aufl. 2004, § 303a Rn. 1; *Schulze-Heiming*, Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls, Diss. Münster, 1995, S. 164.

214 BT-Drs. 10/5058, 34.

215 BT-Drs. 10/5058, 34.

216 *Kühl*, in: Lackner/Kühl, StGB-Kommentar, a. a. O., § 303a Rn. 3.

217 *Hilgendorf*, JuS 1996, 890, 891.

bb) Computersabotage, § 303b StGB

Ein Angriff auf RFID-Systeme könnte auch gem. § 303b StGB strafbewehrt sein. Die Vorschrift schützt das Interesse von Wirtschaft und Verwaltung an der Funktionsfähigkeit ihrer gesamten Datenverarbeitung.²¹⁸ Die Vorschrift setzt voraus, dass der Vorgang einer Datenverarbeitung beeinflusst wird. Der Ausdruck „Datenverarbeitung“ bezeichnet in § 303b StGB den gesamten Arbeitsbereich, der sich auf die Speicherung und Verarbeitung von Daten mittels EDV bezieht. Ein einzelner Datenverarbeitungsvorgang wird nur erfasst, wenn dadurch die betreffende Datenverarbeitung insgesamt beeinträchtigt wird.²¹⁹ Die Tat kann sich folglich nicht auf einzelne RFID-Tags beziehen. Sie ist aber möglich bei einem Angriff auf das Backend eines solchen Systems.

Der Begriff der Datenverarbeitung erfährt eine Einschränkung insofern, als die Datenverarbeitung für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung sein muss. Dies setzt eine solche Komplexität der Datenverarbeitung voraus, dass von ihrem störungsfreien Ablauf die Funktionstüchtigkeit der Einrichtung im Ganzen abhängt.²²⁰ Ein Angriff auf das Backend eines Unternehmens ist also nur dann als Computersabotage zu werten, wenn hiervon seine Funktionstüchtigkeit abhängt. Der Angriff muss eine Störung der Datenverarbeitung verursachen. Dies setzt mehr als eine bloße Gefährdung, nämlich eine nicht unerhebliche Beeinträchtigung des reibungslosen Ablaufs voraus.²²¹ Diese kann zum einen durch eine Datenveränderung nach § 303a Abs. 1 StGB hervorgerufen werden, § 303b Abs. 1 Nr. 1 StGB. Die Computersabotage stellt somit einen qualifizierten Fall der strafbaren Datenveränderung dar, der wegen seiner schwerwiegenden Auswirkungen auf einen wichtigen Datenverarbeitungsvorgang deutlich strenger bestraft werden kann. Zum anderen kann die Störung durch Angriffe auf die Hardware verursacht werden, wenn die Anlage selbst oder einzelne Datenträger zerstört, beschädigt, unbrauchbar gemacht, beseitigt oder verändert werden.

cc) Fälschung beweisheblicher Daten, § 269 StGB

Die Fälschung von Inhalt oder Identität eines RFID-Tags könnte als Fälschung beweisheblicher Daten zu werten sein. Nach § 269 StGB macht sich strafbar, wer zur Täuschung im Rechtsverkehr beweishebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht. Die Fälschung beweisheblicher Daten ist deshalb insoweit geschützt, als ein Vertrauen des Rechtsverkehrs in die Authentizität des Datenbestandes im Hinblick auf dessen unveränderte Herkunft von einem bestimmten Aussteller besteht.²²²

218 *Möhrenschlager*, wistra 1986, 128, 142; *Kühl*, in: Lackner/Kühl, StGB-Kommentar, a. a. O., § 303b Rn. 1.

219 Hilgendorf, JuS 1996, 1082, 1083 m. w. N.

220 *Kühl*, in: Lackner/Kühl, StGB-Kommentar, a. a. O., § 303b Rn. 2.

221 BT-Drs. 10/5058, 36.

222 *Möhrenschlager*, wistra 1986, 128, 134.

Urkunde i.S.d. Strafrechts ist jede verkörperte Erklärung, die ihrem gedanklichen Inhalt nach geeignet und bestimmt ist, für ein Rechtsverhältnis Beweis zu erbringen und die ihren Aussteller erkennen lässt.²²³ Wird ein Tag auf einen Gegenstand aufgebracht, so handelt es sich hierbei, bis auf die visuelle Wahrnehmbarkeit des gespeicherten Inhalts, um eine zusammengesetzte Urkunde, da die beweisheblichen Daten mit dem Trägerobjekt fest zu einer Beweiseinheit verbunden werden.²²⁴ Die Echtheit einer Urkunde bestimmt sich danach, ob alle Angaben in der Urkunde dem vermeintlichen Aussteller auch tatsächlich zuzurechnen sind²²⁵, so dass für die Erklärung im Rechtsverkehr die als Aussteller erscheinende Person tatsächlich haftbar zu machen ist. Unecht ist eine Urkunde daher nicht etwa dann, wenn in ihr inhaltlich Unrichtiges wiedergegeben ist (sog. schriftliche Lüge), sondern wenn die verkörperte Erklärung, sei sie richtig oder falsch, nicht von dem stammt, der in ihr als Aussteller bezeichnet ist. Aussteller des beweisheblichen Ergebnisses eines Datenverarbeitungs- oder Datenspeicherungsvorgangs ist, wem die Gedankenerklärung geistig zuzurechnen ist.²²⁶ Dies ist im hier relevanten Zusammenhang der Verwender des RFID-Systems. Das oben beschriebene Klonen eines Tags würde dem Verwender des ursprünglichen Tags einen gleich lautenden Erklärungsinhalt erneut unterschieben, der diesem auch im Rechtsverkehr zugerechnet würde. Dies entspräche dem Herstellen einer unechten Urkunde, so dass hier eine Strafbarkeit gem. § 269 Abs. 1 StGB vorläge.

Als Verfälschung ist jede nachträgliche Veränderung des gedanklichen Inhalts einer echten Urkunde anzusehen, durch die der Anschein erweckt wird, der Aussteller habe die Erklärung in der Form abgegeben, die sie durch die Verfälschung erlangt hat.²²⁷ Ändert ein Täter also die auf einem Tag gespeicherten Daten, so dass der Anschein entsteht, der reguläre Verwender habe die Daten so abgelegt, so liegt in diesem Fall eine Verfälschung beweisheblicher Daten vor.

223 BGHSt 3, 84; 4, 285; 13, 235; 16, 96.

224 Zu zusammengesetzten Urkunden vgl. Kühl, in: Lackner/Kühl, § 269 Rn. 5 und § 267 Rn. 8.

225 Kühl, in: Lackner/Kühl, § 269 Rn. 6.

226 Kühl, in: Lackner/Kühl, § 269 Rn. 6.

227 OLG Hamm, NJW 1969, 625.

dd) Verändern beweisheblicher Daten, § 274 Abs. 1 Nr. 2 StGB

Das Ablösen eines RFID-Tags von seinem Trägerobjekt könnte eine Straftat nach § 274 Abs. 1 Nr. 2 StGB sein. Danach macht sich strafbar, wer beweishebliche Daten (§ 202a StGB), über die er nicht oder nicht ausschließlich verfügen darf, in der Absicht, einem anderen Nachteil zuzufügen, löscht, unterdrückt, unbrauchbar macht oder verändert. § 274 Abs. 1 Nr. 2 StGB schützt die Integrität und Authentizität (Tathandlungen löschen, unbrauchbar machen und verändern) sowie die Verfügbarkeit (Tathandlung unterdrücken) beweisheblicher Daten und somit die Sicherheit und Zuverlässigkeit des Rechts- und Beweisverkehrs. § 274 Abs. 1 Nr. 2 StGB ist ein Qualifikationstatbestand im Verhältnis zur Datenveränderung gemäß § 303a StGB und stellt das Gegenstück zum Tatbestand der Fälschung beweisheblicher Daten (§ 269 StGB) dar. Während § 269 StGB die positive Schaffung unechter beweisheblicher Daten durch Speicherung und Veränderung regelt, erfasst § 274 Abs. 1 Nr. 2 StGB deren negative Beseitigung durch Löschen, Unterdrücken, Unbrauchbarmachen und Verändern.

Wird also die zusammengesetzte Beweiseinheit aus RFID-Tag und Trägerobjekt z.B. durch Ablösen oder Zerstören des Tags vernichtet, ist dies strafbar gem. § 274 Abs. 1 Nr. 2 StGB.

ee) Computerbetrug, § 263a StGB

Bei der Manipulation von RFID-Systemen kommt auch eine Strafbarkeit gem. § 263a StGB in Betracht. Danach macht sich des Computerbetrugs strafbar, wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst. Geschütztes Rechtsgut ist ausschließlich das Vermögen.²²⁸

Besonders relevant ist dieser Straftatbestand für das Benutzen von Geräten zur Überwindung elektronischer Wegfahrsperrn. In einem entsprechenden Fall hat die Staatsanwaltschaft Konstanz eine Strafbarkeit gem. § 263a Abs. 1 StGB grundsätzlich in Betracht gezogen.²²⁹ Demnach ist die Wegfahrsperrn eines Fahrzeugs als eine Einheit anzusehen, in der durch implementierte Software verschiedene Rechnervorgänge gesteuert werden. Zur Überwindung der Wegfahrsperrn werde die Rechneranlage mit unrichtigen Daten „gefüttert“. Schon die Nutzung eines Kraftfahrzeuges stelle eine vermögenswerte Leistung dar²³⁰, so dass der Tatbestand des § 263a Abs. 1 StGB erfüllt sei.

In dem zu entscheidenden Fall waren die Täter allerdings bereits an der Grenze von Beamten überprüft worden. Dabei stellte sich heraus, dass einer der Täter ein Gerät zur Manipulation und unberechtigten Überwindung der Wegfahrsperrn von hochwertigen BMW-Fahrzeugen mit sich führte.

228 BGHSt 40, 331, 334.

229 AG Konstanz, Strafbefehl vom 7.10.2005, Az. 10 Cs & 0 Js 5031/05 – AK 419/05. Die Staatsanwaltschaft Konstanz hat die Strafverfolgung jedoch gem. § 154a StPO auf die Strafbarkeit gem. §§ 17 Abs. 2 Nr. 1, Abs. 5 UWG i.v.m. §§ 25 Abs. 2, 74 StGB beschränkt.

230 Strafgedanke des § 248b StGB.

Der Mittäter trug fünf Transponder bei sich, die als Fahrzeugschlüssel für Fahrzeuge dienen, bei denen die elektronische, rechner- und softwaregesteuerte Wegfahrsperrung manipuliert wurde. Allein das Mit-sich-Führen des Manipulationsgeräts und der Transponder unterfällt bereits dem Tatbestand des § 263a Abs. 3 StGB. Danach macht sich strafbar, wer eine Straftat nach Abs. 1 vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt. Das Manipulationsgerät enthält nach Ansicht der Staatsanwaltschaft eine entsprechende „Knacksoftware“.

In dem geschilderten Fall erging der Strafbefehl allerdings nicht aufgrund der Strafbarkeit gem. § 263a Abs. 3 StGB, sondern wegen des gemeinschaftlichen Verrats von Geschäfts- und Betriebsgeheimnissen gem. §§ 17 Abs. 2 Nr. 1, Abs. 5 UWG i.V.m. §§ 25 Abs. 2, 74 StGB. Nach § 17 Abs. 2 Nr. 1 UWG macht sich strafbar, wer aus Eigennutz oder zu Gunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, sich ein Geschäfts- oder Betriebsgeheimnis durch Anwendung technischer Mittel oder durch Herstellung einer verkörperten Wiedergabe des Geheimnisses unbefugt verschafft oder sichert. In dem Strafbefehl wird ausgeführt, dass die elektronische Wegfahrsperrung bei hochwertigen Fahrzeugen durch den Hersteller mittels Software und Programmroutinen sowie darauf abgestimmter Hardware realisiert werde. Details dieses Schutzverfahrens seien ein vom Hersteller gehütetes Geschäftsgeheimnis. Das mitgeführte Manipulationsgerät sowie die darauf abgestimmten Transponder verkörperten das entsprechende Geschäftsgeheimnis des Herstellers, das die Täter zu eigenen Zwecken verwenden wollten.

e) Fazit

Zusammenfassend lässt sich sagen, dass die RFID-Technologie zwar neue Risiken für die Verfügbarkeit der Daten, deren Integrität, Vertraulichkeit und Authentizität mit sich bringt. Auf der anderen Seite hat die Untersuchung gezeigt, dass diesen Gefahren durch technische Sicherheitsmaßnahmen begegnet werden kann. Es können Authentifizierungsmechanismen implementiert werden wie beispielsweise ein Passwortschutz. Auch eine weltweit eindeutige Regelung zur Vergabe von Seriennummern kann zum Identitätsschutz von Transpondern beitragen. Zusätzlich bieten sich Verschlüsselungsverfahren und Deaktivierungsmöglichkeiten an. Es bestehen insbesondere für den Bereich der personenbezogenen Daten umfangreiche rechtliche Verpflichtungen zur Datensicherung. Ferner wird die Sicherheit und Integrität von RFID-Systemen auch strafrechtlich geschützt. Eine zusätzliche gesetzliche Regelung für die RFID-Technologie ist nicht erforderlich.

3. SCHUTZ DER VERTRAULICHEN KOMMUNIKATION (FERNMELDEGEHEIMNIS)

Nachdem nun datenschutzrechtliche und sicherheitsrelevante Aspekte der RFID-Technologie untersucht worden sind, soll jetzt überprüft werden, ob die Integrität, Vertraulichkeit und Authentizität von RFID-Systemen auch durch das Fernmeldegeheimnis geschützt sind.

a) Abhörverbot nach § 89 TKG

Im datenschutzrechtlichen Teil wurde festgestellt, dass Produktcodes oder Seriennummern, die auf RFID-Tags gespeichert werden, für sich betrachtet keine personenbezogenen Daten i.S.d. BDSG und datenschutzrechtliche Vorschriften somit nicht anwendbar sind. Hier könnte aber möglicherweise rechtlicher Schutz nach dem Telekommunikationsgesetz (TKG) bestehen.

Im TKG ist das aus Art. 10 GG folgende sog. Fernmeldegeheimnis einfachgesetzlich geregelt. Das Fernmeldegeheimnis nach § 88 TKG schützt die Vertraulichkeit der Telekommunikation. Zu klären ist zunächst, ob der Datenaustausch zwischen RFID-Tag und Reader der Telekommunikation zuzuordnen ist. Telekommunikation ist gem. § 3 Nr. 22 TKG der technische Vorgang des Aussendens, Übermittels und Empfangens von Signalen mittels Telekommunikationsanlagen. Bei den RFID-Komponenten handelt es sich um technische Systeme, die elektromagnetische Signale senden, empfangen und steuern.²³¹ Sie sind daher Telekommunikation i.S.d. Gesetzes und werden folglich grundsätzlich vom Fernmeldegeheimnis geschützt. Der Wahrung des Fernmeldegeheimnisses unterliegen jedoch gem. § 88 Abs. 2 TKG nur die Diensteanbieter, d.h. diejenigen, die ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, § 3 Nr. 6 TKG. Die Verwender von RFID-Systemen bieten jedoch keine Telekommunikationsdienste für Dritte an, so dass § 88 TKG insoweit nicht zur Anwendung gelangt.²³² Die Vertraulichkeit der Kommunikation kann jedoch auch durch Eingriffe Dritter verletzt werden. So ist insbesondere denkbar, dass Tags von Dritten unbefugt ausgelesen werden. Dieser Schutzpflicht dient § 89 TKG, der ein allgemeines Verbot statuiert, Nachrichten abzuhören, die nicht für die empfangene Funkanlage bestimmt sind. Verboten ist des Weiteren gem. S. 2 die Weitergabe des Inhalts oder der Tatsache des unbeabsichtigten Empfangs der Nachricht selbst. Ein Verstoß gegen das Abhörverbot ist gem. § 148 Abs. 1 Nr. 1 TKG strafbar. Fraglich ist, ob RFID-Systeme vom Abhörverbot des § 89 TKG erfasst werden.

²³¹ Müller, DuD 2004, 215, 216.

²³² Die Verwender von RFID-Systemen unterliegen jedoch den datenschutzrechtlichen Bestimmungen, so dass für personenbezogene Daten der Betroffenen ein ausreichender Schutz besteht, s. hierzu bereits ausführlich oben unter IV. 1.

aa) § 89 S. 1 TKG

Der Begriff der Funkanlage wird im 2004 novellierten TKG nicht mehr legaldefiniert. Nach der Definition des § 3 Nr. 4 TKG 1996 sind Funkanlagen elektrische Sende- und Empfangseinrichtungen, zwischen denen die Informationsübertragung ohne Verbindungsleitungen stattfinden kann. An diesem Verständnis hat sich durch die Novellierung des TKG nichts geändert.²³³ RFID-Systeme bestehen aus einer Sende- und einer Empfangseinrichtung. Die Informationsübertragung zwischen diesen beiden Komponenten erfolgt leitungslos per Funk. Sie sind daher als Funkanlage zu qualifizieren. Mit diesen Funkanlagen dürfen keine Nachrichten unbefugt abgehört werden. Der Begriff der Nachricht umfasst jede Information, die zwischen zwei Stellen übermittelt wird. Entscheidendes Merkmal der Nachricht ist der Übermittlungsvorgang.²³⁴ Auf die Geheimhaltungsbedürftigkeit des Informationsgehalts kommt es nicht an. Auch wenig aussagekräftige Signale sind Nachrichten.²³⁵ Geschützt sind folglich nicht nur auf Tags gespeicherte personenbezogene Daten, sondern z.B. auch Seriennummern, wenn diese einen Informationsgehalt aufweisen. Es kommt lediglich darauf an, dass diese Information übermittelt wird, was innerhalb eines RFID-Systems der Fall ist. Fraglich ist allerdings, welchen Informationsgehalt eine Seriennummer oder ein Produktcode für Außenstehende des jeweiligen Unternehmens haben kann. Wenn aus der Nummer Rückschlüsse auf das jeweilige Trägerobjekt, die Handelskette oder möglicherweise die Filiale, in der der Gegenstand gekauft wurde, gezogen werden können, so liegt hierin eindeutig ein Informationsgehalt. Der Nummer kommt damit Nachrichtenwert zu. Aber auch wenn auf den Tags lediglich eine Aneinanderreihung von Zahlen gespeichert ist, ist zu beachten, dass der Nachrichtenbegriff weit auszulegen ist und es auf die Aussagekraft der Information nicht ankommt. Die Information eines gespeicherten Produktcodes ist gerade die Aussage, dass dieses Produkt genau diesen Produktcode hat. Fraglich ist, ob diese weite Auslegung nicht in der Praxis dazu führt, dass eine Vielzahl von RFID-Anwendungen gegen das Abhörverbot verstößt. Im Alltag wird es sich nämlich kaum vermeiden lassen, dass bei einer Abfrage durch ein Lesegerät auch andere Tags ungewollt miterfasst werden. Aus einer Zusammenschau mit § 89 S. 2 TKG ergibt sich jedoch, dass der unbeabsichtigte Empfang einer Nachricht und deren Kenntnisnahme nicht gegen das Abhörverbot verstoßen. Nach § 89 S. 2 TKG ist nämlich die Mitteilung einer Nachricht bei unbeabsichtigtem Empfang unzulässig. Daraus ergibt sich ferner, dass das Nutzen einer unbeabsichtigt empfangenen Nachricht für eigene Zwecke nicht verboten ist²³⁶, so dass auch der unbeabsichtigte Empfang einer Nachricht nicht verboten ist.

233 *Klescewski*, in: Säcker, Berliner Kommentar zum Telekommunikationsgesetz, 2006, § 89 Rn. 4.

234 *Dierlamm*, in: Scheurle/Mayen, Telekommunikationsgesetz, 2002, § 95 TKG Rn. 2.

235 AG Potsdam, ZUM 2000, 166, 167; Müller, DuD 2004, 215, 217; *Klescewski*, in: Säcker, Berliner Kommentar zum Telekommunikationsgesetz, a. a. O., § 89 Rn. 6.

236 *Klescewski*, in: Säcker, Berliner Kommentar zum Telekommunikationsgesetz, a. a. O., § 89 Rn. 14.

Dies entspricht auch dem Normzweck von § 89 TKG, wonach die Vertraulichkeit der Kommunikation vor Eingriffen Dritter geschützt werden soll. Das unbeabsichtigte Empfangen von RFID-Signalen lässt sich aber nicht verhindern, so dass hierin kein Eingriff zu sehen ist. Obwohl eine auf einem Tag gespeicherte Seriennummer Nachrichtenwert haben kann, ist das unbeabsichtigte Empfangen folglich nicht vom Abhörverbot erfasst.²³⁷

Eine Nachricht darf nur abgehört werden, wenn sie für den Betreiber der Funkanlage, Funkamateure i.S.d. Gesetzes über den Amateurfunk, die Allgemeinheit oder für einen unbestimmten Personenkreis bestimmt ist. Die Frage, für wen eine Nachricht bestimmt ist, richtet sich nach der subjektiven Bestimmung des Senders.²³⁸

Abhören ist das Sich-Verschaffen einer Information, die nicht für den Mithörenden gedacht war.²³⁹ Die klassische Konstellation des Abhörens besteht darin, dass sich ein Dritter in die Funkkommunikation zwischen Sender und Empfänger einschaltet. Wird also die Kommunikation zwischen Tag und Reader von einem Dritten mitgehört, so ist ein Abhören i.S.d. Vorschrift zweifelsohne gegeben. Wird ein Transponder jedoch unabhängig von einem regulären Funkvorgang ausgelesen, so regt dieser die Funkkommunikation erst an. Dennoch schließt das eine Anwendung des § 89 TKG nicht aus, da von dem Abhörverbot auch neue Informations- und Kommunikationstechniken erfasst werden sollen.²⁴⁰ Das Auslesen von Transpondern durch Dritte ist von der Interessenlage her vergleichbar mit der klassischen Abhör-Konstellation. Der Wortlaut des § 89 TKG ist nicht darauf beschränkt, dass sich der Abhörende in eine bestehende Funkverbindung einschaltet. Vielmehr soll jeglicher unbefugter Empfang von Nachrichten verboten werden.²⁴¹ Entscheidend ist nur, dass sich der Dritte die spezifischen Eigenschaften der Funktechnik zu Nutze macht, um Nachrichten zur Kenntnis zu nehmen, die nicht für ihn bestimmt sind. Das unbefugte Auslesen eines RFID-Tags ist folglich vom Begriff des Abhörens umfasst.²⁴²

237 So i. E. auch *Müller*, DuD 2004, 215, 217, der Serienkennungen im Wege der teleologischen Reduktion vom Anwendungsbereich des § 86 S. 1 a. F. ausschließt.

238 *Klescewski*, in: Säcker, Berliner Kommentar zum Telekommunikationsgesetz, a.a. O., § 89 Rn. 8; *Müller*, DuD 2004, 215, 217.

239 *Dierlamm*, in: Scheurle/Mayen, Telekommunikationsgesetz, a. a. O., § 95 TKG Rn. 3.

240 *Müller*, DuD 2004, 215, 217.

241 *Müller*, DuD 2004, 215, 217.

242 *Lahner*, Datenschutzrechtliche Probleme beim Einsatz von RFID-Systemen, a. a. O., S. 49; *Müller*, DuD 2004, 215, 217.

bb) § 89 S. 2 TKG

Zum weiteren Schutz der Vertraulichkeit enthält Satz 2 der Vorschrift ein Mitteilungsverbot. Danach ist die Mitteilung des Inhalts von unbefugt abgehörten Nachrichten sowie der Tatsache ihres Empfangs verboten. Empfang ist die Entgegennahme von Worten, Zeichen oder sonstigen Informationen.²⁴³ Mitteilung ist jede Art von mündlicher oder schriftlicher Bekanntgabe. Die Mitteilung ist auch bei unbeabsichtigtem Empfang unzulässig, § 89 Satz 2 TKG. Aus dieser Regelung ergibt sich ferner, dass das Nutzen einer unbeabsichtigt empfangenen Nachricht für eigene Zwecke nicht verboten ist.²⁴⁴ Auch der unbeabsichtigte Empfang einer Nachricht und deren Kenntnisnahme verstoßen nicht gegen das Abhörverbot. Allerdings greift hier der durch § 89 S. 2 TKG angeordnete Nachsorge-schutz, d.h. dass unbeabsichtigt empfangene Daten nicht weitergegeben werden dürfen.

b) Strafbarkeit gem. § 148 Abs. 1 Nr. 1 TKG**aa) Objektiver Tatbestand**

Hört jemand unbefugt die Kommunikation zwischen einem RFID-Tag und einem Reader ab oder liest jemand unbefugt ein Tag aus, so kann dies auch als Straftat gem. § 148 Abs. 1 Nr. 1 TKG gewertet werden. Danach macht sich strafbar, wer entgegen § 89 S. 1 oder 2 TKG eine Nachricht unbefugt mittels einer Funkanlage abhört oder den Inhalt einer unbefugt empfangenen Nachricht oder die Tatsache ihres Empfangs einem anderen mitteilt. Die Tat kann nur gegen den Willen des Senders der Nachricht begangen werden, da die Frage, für wen sie bestimmt ist, subjektiv zu beurteilen ist.²⁴⁵ Willigt der Sender in den Empfang der Nachricht ein, so handelt es sich hierbei um ein tatbestands-ausschließendes Einverständnis.²⁴⁶

bb) Subjektiver Tatbestand

§ 148 TKG ist eine in einem Nebengesetz enthaltene materielle Strafrechtsnorm, so dass gem. Art. 1 Abs. 1 EGStGB die Vorschriften des Allgemeinen Teils des StGB uneingeschränkt gelten. Folglich ist nur die vorsätzliche Begehung strafbar, da das fahrlässige Handeln nicht ausdrücklich mit Strafe bedroht ist, § 15 StGB.

cc) Versuchsstrafbarkeit und Vollendung

Der Versuch ist nicht strafbar, § 23 Abs. 1 StGB. Die erste Tatbestandsalternative ist allerdings bereits mit dem Abhören der ersten Sequenz der Nachricht vollendet.²⁴⁷ Auch das Mitteilen von Informationen ist bereits dann vollendet, wenn der Empfänger nur den Anfang der Mitteilung erhalten hat.²⁴⁸

243 *Dierlamm*, in: Scheurle/Mayen, Telekommunikationsgesetz, a. a. O., § 95 TKG Rn. 3.

244 *Klescewski*, in: Säcker, Berliner Kommentar zum Telekommunikationsgesetz, a. a. O., § 89 Rn. 14.

245 Vgl. oben unter IV 3. a) aa).

246 *Klescewski*, in: Säcker, Berliner Kommentar zum Telekommunikationsgesetz, a. a. O., § 148 Rn. 7.

247 Entsprechend zu § 201 StGB: Lenckner, in: Schönke/Schröder, Kommentar zum StGB, 27. Aufl. 2006 § 201, Rn. 36.

248 *Büchner*, in: Beck'scher TKG-Kommentar, 2000, § 95 TKG Rn. 4.

dd) Konkurrenzen und Strafraumen

Wer eine Nachricht sowohl unbefugt abhört als auch Informationen darüber mitteilt, begeht nur eine Tat, da es sich um unselbstständige Tatbestandsalternativen handelt.²⁴⁹ Die Tat wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Bei § 148 TKG handelt es sich um ein Officialdelikt, d.h., zur Strafverfolgung ist ein vorheriger Strafantrag nicht erforderlich.

c) Ausspähen von Daten, § 202a StGB

Auf RFID-Tags gespeicherte Daten könnten auch dem strafrechtlichen Schutz des § 202a StGB unterfallen. Danach macht sich strafbar, wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft. § 202a StGB schützt die Vertraulichkeit der Daten. Gemeint ist damit die aus dem Recht am gedanklichen Inhalt folgende Befugnis, andere von ihrer Kenntnisnahme auszuschließen, und zwar unabhängig von den Eigentumsverhältnissen am Datenträger oder davon, ob es sich bei den Daten tatsächlich um Geheimnisse handelt.²⁵⁰ Enthält ein Datenträger z.B. die Adresse eines Betroffenen, so ist das Ausspähen dieser Daten unabhängig davon strafbar, ob die Adresse geheim oder allgemein bekannt ist oder ob sie auf dem Datenträger des Betroffenen oder eines Dritten gespeichert ist.

aa) Tatobjekt

Der zentrale Begriff des § 202a StGB ist das Datum. § 202a StGB stellt keine besonderen inhaltlichen Anforderungen an die geschützten Daten. So muss es sich insbesondere nicht um personenbezogene Daten handeln. § 202a Abs. 2 StGB grenzt den Begriff lediglich dahingehend ein, dass Daten i.S.d. § 202a Abs. 1 StGB nur solche sind, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.²⁵¹ Geschützt werden folglich auch Tags, auf denen ausschließlich Seriennummern oder Produktcodes gespeichert sind.

§ 202a StGB schützt die Daten nur, wenn sie nicht für den Täter bestimmt sind. Dies sind sie dann nicht, wenn sie nach dem Willen des Berechtigten nicht in den Herrschaftsbereich des Täters gelangen sollen.²⁵² Zudem müssen die Daten gegen unberechtigten Zugang besonders gesichert sein. Besondere Sicherungen i.S.d. § 202a StGB sind Vorkehrungen, die objektiv geeignet und subjektiv nach dem Willen des Berechtigten dazu bestimmt sind, den Zugriff auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren.²⁵³ Es werden sowohl mechanische Sicherungen wie z.B. verschlossene Behältnisse als auch elektronische Sicherungen wie z.B. Passwörter oder Verschlüsselungsmechanismen erfasst.

249 *Büchner*, in: Beck'scher TKG-Kommentar, a. a. O., § 95 TKG Rn. 6.

250 *Hilgendorf*, JuS 1996, 509, 511; *Lenckner*, in: Schönke/Schröder, § 202a, Rn. 1.

251 Zu den einzelnen Begriffsmerkmalen und zur daran geübten Kritik siehe *Lenckner*, in: Schönke/Schröder, § 202a, Rn. 4.

252 *Möhrenschlager*, wistra 1986, 128, 140.

253 *Lenckner*, in: Schönke/Schröder, § 202a, Rn. 7.

Auf RFID-Tags gespeicherte Daten unterliegen daher nur dann dem strafrechtlichen Schutz des § 202a StGB, wenn sie durch ein kryptografisches Verfahren oder einen Passwortschutz besonders gesichert sind. Dies wird bei im Handel verwendeten Tags, auf denen lediglich eine Seriennummer oder ein Produktcode gespeichert wird, in der Regel nicht der Fall sein, da die Produktionskosten bei komplizierteren Schutzmaßnahmen für den massenhaften Gebrauch zu hoch wären.

bb) Taterfolg

Der Taterfolg liegt in dem Verschaffen der Daten für sich oder für einen anderen. Dies erfordert das Herstellen der eigenen Herrschaft oder derjenigen eines anderen über die Daten. Dies ist zum einen immer dann der Fall, wenn der Täter oder der Dritte von ihnen Kenntnis genommen hat. Zum anderen genügt auch bereits die bloße Möglichkeit der Kenntnisnahme, wenn der Täter einen Datenträger in seine oder des Dritten Verfügungsgewalt bringt oder wenn er die Daten auf einem eigenen Datenträger oder dem eines Dritten speichert.²⁵⁴ Besonderheiten ergeben sich, wenn die Daten verschlüsselt sind. In diesem Fall hat sich der Täter die Daten erst dann verschafft, wenn sie entschlüsselt wurden und im Klartext vorliegen.²⁵⁵

d) Fazit

Die Vertraulichkeit der Kommunikation innerhalb von RFID-Systemen ist auch durch das Fernmeldegeheimnis geschützt. Vom Abhörverbot des § 89 TKG ist jedoch nur das beabsichtigte Auslesen von Transpondern betroffen. Zusätzlich wird die Vertraulichkeit durch die Straftatbestände der §§ 148 Abs. 1 Nr. 1 TKG und 202a StGB abgesichert. Insgesamt erscheint daher die aktuelle Gesetzeslage ausreichend, um die derzeit mit RFID verbundenen Risiken zu bewältigen.

²⁵⁴ *Lenckner*, in: Schönke/Schröder, § 202a, Rn. 10.

²⁵⁵ *Schmitz*, JA 1995, 483; a. A. Hilgendorf, JuS 1996, 702, 705.

V. RECHTSPOLITISCHE DEBATTE

1. TECHNOLOGISCHER WANDEL UND DAS PRINZIP DER VERANTWORTUNG

Die moderne Informationsgesellschaft befindet sich in einem ständigen technologischen Wandel. Die Geräte der neuen digitalen Welt sind intelligent: Sie können hören, lesen, sehen und Auskunft geben. Die RFID-Technologie, die auch als Basistechnologie für das sog. „Internet der Dinge“ gilt, ermöglicht es, den Umschlag von Waren und Dienstleistungen weiter zu beschleunigen und besser auf die Bedürfnisse der Unternehmen und Verbraucher einzustellen. Einschneidende Veränderungen sind beispielsweise für den Handel, die Logistik und den Sicherheitsbereich zu erwarten.²⁵⁶

Keine neue Technik ist ohne Risiken. Da die RFID-Technologie das Erfassen und Auslesen von Daten erleichtert, besteht die Befürchtung, dass das Recht auf informationelle Selbstbestimmung nicht hinreichend respektiert wird. Entsprechend kamen in letzter Zeit verschiedentlich Forderungen nach einer Weiterentwicklung und Modernisierung des 2001 nach europäischen Maßstäben neu gefassten Bundesdatenschutzgesetzes auf. Kritiker befürchten, dass die RFID-Technologie von Unternehmen zum Erstellen von Kunden- oder Persönlichkeitsprofilen missbraucht werden könnte. Auch Befürchtungen wie der gläserne Bürger und das Entstehen eines Überwachungsstaats werden in diese Diskussion mit eingebracht. Aber auch auf mögliche Gefahren für die Datensicherheit wird hingewiesen. Die neuen Techniken könnten von Dritten angegriffen und ihre Funktionen könnten gestört werden. Zudem könnten Unbefugte die auf den RFID-Tags gespeicherten Daten ausspionieren.

Vor diesem Hintergrund wird ein breiter Einsatz von RFID von vielen Verbrauchern und insbesondere Verbraucherverbänden abwartend oder gar skeptisch beurteilt. Verstärkt wird ihr Misstrauen durch Pressemeldungen, die über spektakuläre Anwendungen berichten. So wird RFID offenbar zu zweifelhaften Zwecken eingesetzt, wobei die Überwachung von Menschen nicht nur möglich, sondern teilweise auch Zweck des Technologieeinsatzes ist. Ein Beispiel dafür ist eine US-amerikanische Firma, die ihre Mitarbeiter dazu anhält, sich RFID-Chips in den Körper injizieren zu lassen, um so das Verfahren der Zutrittskontrollen für Kontrollräume zu verbessern.²⁵⁷ Auch der Einsatz von RFID in einigen Schulen zur Überprüfung der Anwesenheit ihrer Schüler stimmt bedenklich.²⁵⁸ Diese Beispiele belegen, dass sowohl private als auch öffentliche Einrichtungen unbedacht und verantwortungslos mit den Möglichkeiten einer neuen Technologie umgehen können. Festzuhalten ist aber auch, dass es sich hierbei um Einzelfälle handelt. Die massenhafte Verwendung der Technologie im Handel, aber auch in anderen Bereichen, stellt sich weit weniger Aufsehen erregend dar. In einer Großzahl von Anwendungen werden gar keine personenbezogenen Daten erhoben oder verarbeitet, so dass insofern auch keine Überwachung von Personen stattfinden kann.

²⁵⁶ Zu den zentralen Anwendungsfeldern von RFID s. unter III.

²⁵⁷ Vgl. heise online, Meldung vom 10.2.2006, abrufbar unter <<http://www.heise.de/newsticker/meldung/69438>>.

²⁵⁸ Vgl. heise online, Meldung vom 7.2.2005, abrufbar unter <<http://www.heise.de/newsticker/meldung/56117>> und Meldung vom 18.2.2005, abrufbar unter <<http://www.heise.de/newsticker/meldung/56562>>.

Mit den Risiken einer neuen Technik wächst auch die Verantwortung für ihren sozialverträglichen Einsatz. Gefordert ist daher eine Beachtung ethischer Werte durch die Handelnden. Und dies bedeutet für RFID, dass insbesondere den Belangen des Datenschutzes, der Datensicherheit und des Fernmeldegeheimnisses hinreichend Rechnung getragen werden muss.

2. HOHES SCHUTZNIVEAU DURCH BESTEHENDE RECHTLICHE VORKEHRUNGEN

Im Unterschied z.B. zu den Vereinigten Staaten wird es in dieser Bundesrepublik als eine gewichtige Aufgabe des Staates angesehen, für ein angemessenes Niveau an Datenschutz, Schutz des Fernmeldegeheimnisses und Datensicherheit zu sorgen. Dementsprechend enthält unsere Rechtsordnung zahlreiche Vorgaben, um diese Schutzziele zu gewährleisten. Das deutsche Datenschutz- und Datensicherheitsrecht weist im internationalen Vergleich ein besonders hohes Schutzniveau auf. Der rechtliche Rahmen für den Einsatz von RFID ist im Einzelnen im Teil IV dieser Abhandlung untersucht worden. Hierbei hat sich ergeben, dass im Hinblick auf die in der Bundesrepublik von RFID ausgehenden potenziellen Risiken keine Regelungslücken erkennbar sind.²⁵⁹ Diese Sichtweise wird auch von der Bundesregierung geteilt.²⁶⁰

3. OPTIMIERUNG DES SCHUTZINSTRUMENTARIUMS

In der rechtspolitischen Diskussion um einen möglichst verträglichen Einsatz von RFID wird überwiegend für eine Optimierung des bestehenden Instrumentariums plädiert. Hierbei geht es darum, die Möglichkeiten des bestehenden Rechtsrahmens auszuschöpfen und diese auf die neuen Anforderungen einzustellen. Ziel der Vorschläge ist es auch, auf die Befürchtungen, durch RFID überwacht und durchleuchtet zu werden, einzugehen. Denn schon allein das „Sich-Beobachtet-Fühlen“ reicht aus, um den Einzelnen in seinem Freiheitsempfinden zu beeinträchtigen. Um diesen Einstellungen und zum Teil auch Ängsten zu begegnen, bietet es sich vielfach an, Vorkehrungen zu ergreifen, die über das bestehende gesetzlich festgelegte Schutzniveau hinausgehen. Die vorgeschlagenen Maßnahmen reichen daher von einer Verbesserung der Transparenz des RFID-Einsatzes und seiner Folgen bis zu einer Verbesserung des Datenschutzes durch Technik und Selbstverpflichtung.

259 So z.B. das Positionspapier des FoeBud, das sich für ein gesetzliches Verbot einiger Anwendungen von RFID ausspricht, im Internet ist das Dokument abrufbar unter <<http://www.foebud.org/rfid/positionspapier.pdf>>.

260 Vgl. RDV 2004, 196, 197 zur Kleinen Anfrage der FDP-Fraktion nach den Gefahren eines Missbrauchs von Radio Frequency Identification Chips.

a) Kennzeichnung von Produkten mit RFID

Vor diesem Hintergrund diskutieren Politik und Wirtschaft zurzeit, ob alle mit RFID-Chips versehenen Produkte zu kennzeichnen sind, und zwar auch dann, wenn keine gesetzliche Kennzeichnungspflicht für Produkte mit RFID-Tags besteht, weil darauf keine personenbezogenen Daten gespeichert sind und auch kein Personenbezug hergestellt werden soll. Nur so könne die Akzeptanz beim Kunden hergestellt bzw. gesteigert werden.²⁶¹ Die Industrie könne so zeigen, dass sie verantwortungsvoll mit Verbraucherrechten umgehe.

Beispielsweise könnte jedes Produkt bzw. jede Verpackung, die mit einem RFID-Chip versehen ist, durch Aufbringung eines besonderen Logos gekennzeichnet werden. Die Verbraucher können z.B. darüber informiert werden, wie das Tag entfernt, ausgeschaltet oder unbrauchbar gemacht werden kann. Außerdem sollten Informationen über die auf dem Chip gespeicherten Daten für die Konsumenten leicht zugänglich gemacht werden. Dadurch können die Kunden mit dem Logo vertraut gemacht, die Technologie erklärt und ihre Vorteile aufgezeigt werden. Die Aufklärungspflichten sollten sich auch auf mögliche Sicherheitsrisiken beziehen. Den Verbrauchern muss klar sein, dass Tags theoretisch von Dritten ausgelesen werden können, dass diese aber in der Regel mit den gespeicherten Zahlencodes keine Information über das jeweilige Produkt oder über den Kunden erhalten. Im Rahmen der Selbstverpflichtung von EPCglobal ist eine solche Kennzeichnungspflicht für die beteiligten Unternehmen vorgesehen.²⁶²

Eine andere Möglichkeit zur Herstellung von Transparenz wäre die Kennzeichnung von Verkaufsräumen, in denen Waren mit RFID-Chips verkauft werden, durch Hinweisschilder. Informationstafeln im Eingangsbereich, die die Verwendung von RFID näher erläutern, könnten diese Hinweispflichten sinnvoll ergänzen.

b) Auskunft über gespeicherte Informationen

Um gespeicherte Daten für Betroffene transparent zu machen, sollte diesen die Möglichkeit eingeräumt werden, die gespeicherten Informationen einzusehen. Werden personenbezogene Daten gespeichert, so müssen sowohl Behörden (§ 19a BDSG) als auch private Stellen eine solche Einsichtnahme gewähren. Aber auch wenn keine personenbezogenen Daten, sondern lediglich ein elektronischer Produktcode betroffen ist, könnte eine Auskunftsverpflichtung dazu beitragen, das Vertrauen des Kunden in die neue Technologie zu stärken. Er könnte sich nämlich selbst vergewissern, dass keine geheimhaltungsbedürftigen Informationen auf dem Tag gespeichert sind. In Supermärkten oder sonstigen Geschäften, in denen RFID-Transponder verwendet werden, könnten am Ausgang beispielsweise Leseterminale aufgestellt werden, an denen sich die Kunden bei Bedarf über die gespeicherten Daten informieren können. Dann könnten sie selbst bestimmen, ob sie den Mikrochip aktiviert lassen wollen, um später ggf. Gewährleistungsrechte auch ohne Kassenbonn geltend machen zu können, oder ob sie die gespeicherten Daten löschen bzw. den RFID-Chip deaktivieren wollen.²⁶³

²⁶¹ Holzmagell/Bonnekoh, MMR 2006, 17, 23.

²⁶² Hierzu näher unter V. 3. e).

²⁶³ Zu Letzterem sogleich unter V. 3. c).

c) Deaktivierung von Tags und Verhinderung ihres Auslesens

Des Weiteren kommt eine Deaktivierung der Transponder auf Produktverpackungen oder Etiketten infrage. Dann könnten die Verbraucher im Einzelfall entscheiden, wie sie mit den Tags umgehen möchten. Sie wären befugt, die Chancen und Risiken der Nutzung von RFID selbst abzuwägen. Sie könnten zudem den Transponder zeitweise deaktivieren, um punktuelle Risiken eines Missbrauchs zu vermeiden und damit ganz gezielt das Sicherheitsniveau an die Gefährdungslage anzupassen. Im Handel werden zum Teil bereits Deaktivierungsmöglichkeiten angeboten. Bei Durchführung dieses Kill-Befehls wird der Chip im Augenblick noch dauerhaft unbrauchbar gemacht, so dass auch für den Kunden nützliche Informationen verloren gehen. Mittlerweile werden aber auch RFID-Chips entwickelt, bei denen der Kunde bei Bedarf die Verbindung zwischen Chip und Antenne durch einfaches Abreißen trennen und so die Aussendung von Funksignalen unterbinden kann. Dies hat den Vorteil, dass die gespeicherten Daten im Bedarfsfall aus sehr geringer Entfernung wieder gelesen werden können, sofern sie noch einmal benötigt werden.²⁶⁴

d) Auditierung und Gütesiegel

Gefordert wird von einigen Verbraucherschutzverbänden, dass die Einführung und Verwendung von RFID-Systemen auf ihre Verbraucherschutzverträglichkeit überprüft werden. Dies könnte durch ein Auditierungsverfahren geschehen. Als Instrument der Selbstkontrolle bietet es die Möglichkeit, freiwillig ein Managementsystem zum Schutz persönlicher Daten, der Datensicherheit oder des Fernmeldegeheimnisses einzurichten.²⁶⁵ Die autonome Selbstkontrolle soll das Verantwortungsbewusstsein der Datenverarbeiter stärken und den Wettbewerb um das beste Schutzkonzept stimulieren. Zu beachten ist aber auch, dass die Auditierungen und die Vergabe von Gütesiegeln einen zusätzlichen Kostenfaktor und erhöhten Bürokratieaufwand bedeuten können.

§ 9a BDSG sieht explizit die Einrichtung eines Datenschutzaudits vor. Danach können datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die genauen Anforderungen dafür sollen in einem besonderen Gesetz geregelt werden.

Zudem sind Gütesiegel geeignet, das Vertrauen der Verbraucher zu stärken. So könnten die Kunden selbst entscheiden, welchem Unternehmen sie ihre Daten anvertrauen wollen und welchem nicht. In Nordrhein-Westfalen besteht z.B. aufgrund der Verordnung zum „Datenschutz-Gütesiegel“²⁶⁶ die Möglichkeit, dass Gütesiegel für IT-Produkte verliehen werden, wenn das Produkt mit den Vorschriften über den Datenschutz und die Datensicherheit vereinbar ist. Besonderer Wert wird dabei auf die Aspekte Datenvermeidung, Datensparsamkeit, Datensicherheit und Revisionsfähigkeit gelegt.

²⁶⁴ S. hierzu bereits unter IV. 2. b) dd).

²⁶⁵ *Roßnagel*, in: *Roßnagel*, Handbuch Datenschutzrecht, a. a. O., 3.7, Rn. 1.

²⁶⁶ Landesverordnung über ein Datenschutzaudit – DSAVO, GVBl. I, 51.

e) Selbstverpflichtungserklärungen

Um das Vertrauen in die RFID-Technologie zu fördern, können die Anwender sich überdies zu einer Einhaltung eines ggf. über die gesetzlichen Vorgaben hinausgehenden Schutzniveaus verpflichten. Beispielsweise gibt es derzeit für die erwähnten Kennzeichnungspflichten und Deaktivierungsmöglichkeiten keine rechtlichen Vorgaben. Es bietet sich daher an, diese im Wege der Selbstverpflichtung in die Praxis umzusetzen.

Einen Schritt in diese Richtung stellen die Standards für das Electronic Product Code (EPC)-Netzwerk der EPCglobal, Inc. dar. EPCglobal ist eine im Jahre 2003 gegründete Non-profit-Organisation, die für den Handel Selbstverpflichtungserklärungen ausarbeitet. Ihre Richtlinien sehen z.B. vor:²⁶⁷

1. Information

Ist ein Produkt oder eine Verpackung mit einem EPC versehen, wird der Konsument darüber informiert. Dies geschieht durch ein EPCglobal-Logo oder -Kennzeichen auf der entsprechenden Einheit.

2. Wahlmöglichkeit

Konsumenten erhalten Informationen, wie der Transponder auf den erworbenen Produkten entfernt, ausgeschaltet oder unbrauchbar gemacht werden kann. Es ist anzunehmen, dass der Transponder bei den meisten Produkten Bestandteil der Umverpackung sein wird oder sich anderweitig unbrauchbar machen lässt. EPCglobal verpflichtet sich, neben anderen Förderern der EPC-Technologie, weitere kostengünstige und sichere Alternativen für den Endverbraucher zu entwickeln.

3. Aufklärung

Informationen über EPC und RFID und entsprechende Anwendungen werden für Verbraucher leicht erhältlich sein. Dies gilt ebenso für Informationen über den Fortschritt dieser Technologie. Unternehmen, die Transponder auf Endverbrauchereinheiten verwenden, werden in angemessener Weise kooperieren, um Konsumenten mit dem EPC-Logo vertraut zu machen, ihnen die Technologie zu erläutern und die Vorteile aufzuzeigen.

²⁶⁷ Die Richtlinien sind im Internet abrufbar unter <<http://www.gs1-germany.de/internet/content/produkte/epcglobal/e140/e144>>.

4. Aufzeichnung, Vorbehalt und Sicherheit:

Der EPC enthält, sammelt oder speichert keine personenbezogenen Daten. Analog zur herkömmlichen Strichcode-Technik werden EPC-spezifische Daten durch die Unternehmen gemäß den geltenden Rechtsvorschriften erhoben, gesammelt, gespeichert, gepflegt und geschützt. Im Einklang mit allen anzuwendenden Gesetzen informieren die Unternehmen über Haltung, Nutzung und Schutz jeglicher personenbezogenen Daten in Verbindung mit dem Einsatz des EPC.

Auch auf nationaler Ebene gibt es Aktivitäten im Bereich der Selbstregulierung, so z.B. im Rahmen eines vom Bundeswirtschaftsministerium unterstützten Runden Tisches mit Vertretern aus Handel und Konsumgüterindustrie sowie Daten- und Verbraucherschützern.

4. Zukünftige Entwicklung

Es lässt sich derzeit nicht im Einzelnen abschätzen, ob durch einen breiten Einsatz von RFID neue Risiken im Bereich des Datenschutzes auf uns zukommen. Soweit auf neue Situationen nicht mehr im Wege der Optimierung des bestehenden Instrumentariums oder durch Selbstverpflichtung angemessen reagiert werden kann, kommt dann ein Handeln des Gesetzgebers in Betracht.

Um auf die vorausgesagte Datenflut und die Möglichkeit ihrer Auswertung durch neue Methoden des Data-Mining zu reagieren, ist kürzlich vorgeschlagen worden, zukünftig zwischen einer zielgerichteten und einer ungezielten Erhebung von Daten zu differenzieren. Das Erheben von Daten wird vom Gesetz definiert als das Beschaffen von Daten über den Betroffenen (§ 3 Abs. 3 BDSG).²⁶⁸ Erste Voraussetzung ist also, dass die betreffende Stelle objektiv Kenntnis von den Daten erhält oder Verfügungsmacht über diese begründet. Allerdings erfüllt nicht jedes Erhalten oder Empfangen die Voraussetzungen des Beschaffens. Hinzukommen muss ein aktives Handeln, das von einem entsprechenden zurechenbaren Willen der handelnden Person getragen ist.²⁶⁹ Die bloß objektive Begründung der Verfügungsmacht über die Daten reicht nicht aus. Dies ergibt sich bereits daraus, dass das Gesetz selbst Fälle der Speicherung von Daten und damit eine Verfügungsgewalt über diese voraussetzt, ohne dass zuvor eine Erhebung vorausgegangen sein muss.²⁷⁰ Ein Erheben personenbezogener Daten liegt daher nur dann vor, wenn die Daten zielgerichtet beschafft werden.²⁷¹

Bei der automatischen Identifikation erfolgt unvermeidlich die Erfassung der Kennungen aller RFID-Chips in der Reichweite des Lesegeräts; sie kann nicht auf bestimmte Tags beschränkt werden.²⁷² In der Alltagsanwendung von RFID wird es demzufolge wahrscheinlich sein, dass bei einer Abfrage durch ein Lesegerät auch andere Tags ungewollt miterfasst werden. Rein rechtlich betrachtet stellt sich die Situation wie folgt dar: Ein solches ungewolltes Auslesen von RFID-Tags ist keine Datenerhebung i.S.d. BDSG.²⁷³ Werden diese Daten dann allerdings weiter verwendet, so finden die datenschutzrechtlichen Bestimmungen Anwendung. Die verantwortliche Stelle darf sich nicht auf

268 Hierzu bereits ausführlich unter IV. 1. c) aa).

269 *Dammann*, in: Simitis Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 3 Rn. 108.

270 So in § 14 Abs. 1 S. 2 BDSG, vgl. dazu *Dammann*, in: Simitis Kommentar zum Bundesdatenschutzgesetz, a. a. O., § 3 Rn. 108.

271 *Gola/Schomerus*, BDSG-Kommentar, a. a. O., § 3 Rn. 24; hierzu auch bereits unter IV. 1. c) aa).

272 *Müller*, DuD 2004, 215, 217.

273 Diese Problematik wurde bereits unter IV. 1. c) aa) angesprochen.

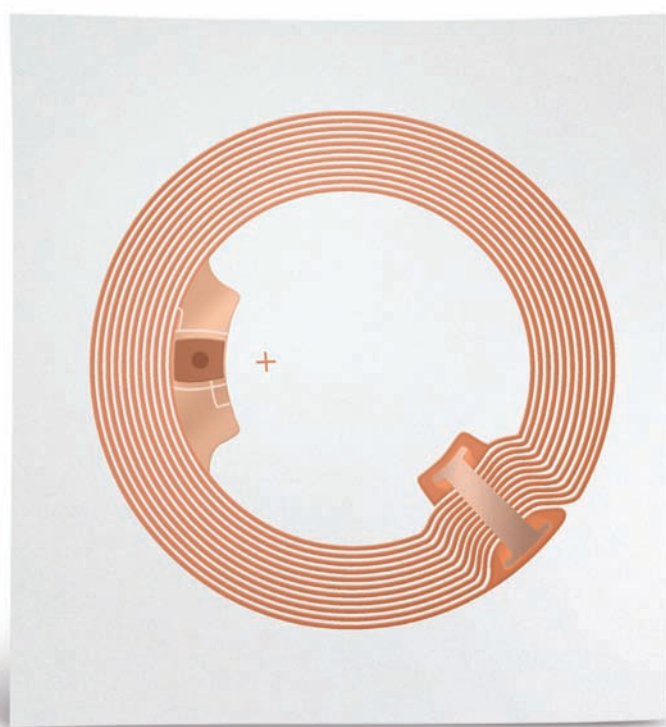
sie berufen und darf sie nicht speichern. Sind sie bereits gespeichert, so sind die Daten unverzüglich zu löschen, § 20 Abs. 2 Nr. 1, § 35 Abs. 2 Nr. 1 BDSG.²⁷⁴

In tatsächlicher Hinsicht kann aber festgestellt werden, dass sich durch den Einsatz der RFID-Technologie das Risiko des ungezielten Datenempfangs erhöht. So entsteht auch nach Ansicht des Bundesdatenschutzbeauftragten durch neue technische Infrastrukturen die Frage, „wer eigentlich für all die anfallenden Daten verantwortlich ist“.²⁷⁵ Seiner Auffassung nach müsse das BDSG diese Frage in Zukunft aufgreifen und zwischen zielgerichteter Datensammlung und der ungezielten Datenerhebung differenzieren. Gerade mit den ungezielt erhobenen Daten müsse sehr viel sorgfältiger umgegangen werden, als es bisher der Fall sei. Welche Regeln hierfür dann im Einzelnen gelten sollen, bliebe zu diskutieren.

Derzeit macht es wenig Sinn, auf diese noch weitgehend unbestimmten Möglichkeiten mittels eines Gesetzes reagieren zu wollen. Auch ist es kaum zweckmäßig, jetzt isoliert geltende gesetzliche Vorkehrungen für die RFID-Technologie zu schaffen. Der technologische Wandel wird sich immer weiter fortsetzen und die Steuerungsfähigkeit des Rechts würde überfordert, wollte man auf jeden Trend mit Änderungen des Gesetzes reagieren. Vielmehr gilt es derzeit insbesondere das flexible Instrumentarium des Datenschutzrechts auf die neuen Herausforderungen einzustellen.

274 *Schild*, in: Roßnagel, Handbuch Datenschutzrecht, a. a. O., 4.2, Rn. 47.

275 *Schaar*, „Überwachung im Alltag ist jetzt möglich“, Interview in der Berliner Zeitung vom 6. Januar 2006; abrufbar unter <<http://www.berlinonline.de/berliner-zeitung/politik/515174.html?2006-01-06>>.



VI. ZUSAMMENFASSUNG

RFID ist eine zukunftssträchtige Technologie, die in verschiedensten Anwendungsbereichen zum Einsatz kommen kann. Die Einsatzgebiete reichen von der Tierkennzeichnung über die neuen Reisepässe, den Einsatz im Freizeitbereich und im Gesundheitswesen bis hin zum Handel. Speziell die Anwendung im Bereich des Einzelhandels ist Gegenstand der öffentlichen Diskussion, da hier der Verbraucher unmittelbar mit den Mini-Transpondern in Berührung kommt.

Datenschutzrechtliche Vorschriften finden im Zusammenhang mit RFID Anwendung, wenn personenbezogene Daten unmittelbar auf dem Tag gespeichert werden oder wenn eine Verknüpfung über das Tag mit solchen Daten z.B. über eine Kundenkarte möglich ist. Ist auf einem Tag lediglich ein elektronischer Produktcode gespeichert, so handelt es sich hierbei mangels Bestimmbarkeit einer Person nicht um ein personenbezogenes Datum und das Datenschutzrecht ist somit nicht anwendbar. Ist das BDSG anwendbar, so ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach § 4 Abs. 1 BDSG nur dann zulässig, wenn der Betroffene eingewilligt hat oder das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet. Als ein solcher Erlaubnistatbestand ist vor allem § 28 Abs. 1 S. 1 BDSG in Erwägung zu ziehen. Auch die weiteren datenschutzrechtlichen Grundsätze wie das Prinzip der Erforderlichkeit, der Transparenz- und der Zweckbindungsgrundsatz sind zu beachten. Werden mobile Speichermedien eingesetzt, bestehen zusätzliche Unterrichtungspflichten des Verwenders nach § 6c BDSG. Dies ist z.B. bei der Verwendung von Kundenkarten der Fall.

Der Verstoß gegen datenschutzrechtliche Vorschriften ist bußgeld- und ggf. strafbewehrt. Nach § 43 Abs. 2 Nr. 1 BDSG ist das vorsätzliche oder fahrlässige unbefugte Erheben oder Verarbeiten personenbezogener Daten, die nicht allgemein zugänglich sind, eine Ordnungswidrigkeit und kann mit einer Geldbuße von bis zu 250.000€ geahndet werden. Wird eine Handlung nach § 43 Abs. 2 Nr. 1 BDSG gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begangen, handelt es sich gem. § 44 Abs. 1 StGB um eine Straftat, die mit Freiheitsstrafe von bis zu zwei Jahren oder mit Geldstrafe bestraft werden kann.

Die RFID-Technologie bringt potenzielle Risiken für die Datensicherheit mit sich. Theoretisch sind Angriffe auf die Verfügbarkeit der Daten, deren Integrität, Vertraulichkeit und Authentizität möglich. Allerdings kann diesen Gefahren durch technische Sicherheitsmaßnahmen begegnet werden. Es können Authentifizierungsmechanismen implementiert werden wie beispielsweise ein Passwortschutz. Auch eine weltweit eindeutige Regelung zur Vergabe von Seriennummern, Verschlüsselungsverfahren und Deaktivierungsmöglichkeiten können zum Schutz von auf Transpondern gespeicherten Daten beitragen. Insbesondere für den Bereich der personenbezogenen Daten bestehen umfangreiche rechtliche Verpflichtungen zur Datensicherung. Zentrale Norm ist hier § 9 BDSG i.V.m.

der Anlage zu § 9 BDSG. Ferner werden die Sicherheit und Integrität von RFID-Systemen auch strafrechtlich durch die Tatbestände der Datenveränderung (§ 303a StGB), der Computersabotage (§ 303b StGB), der Fälschung beweiserheblicher Daten (§ 269 StGB), das Verändern beweiserheblicher Daten (§ 274 Abs. 1 Nr. 2 StGB) und des Computerbetrugs (§ 263a StGB) geschützt. Die Vertraulichkeit der Kommunikation innerhalb von RFID-Systemen wird ferner durch das Fernmeldegeheimnis geschützt. Vom Abhörverbot des § 89 TKG ist jedoch nur das beabsichtigte Auslesen von Transpondern betroffen. Zusätzlich wird die Vertraulichkeit durch die Straftatbestände der §§ 148 Abs. 1 Nr. 1 TKG und 202a StGB abgesichert.

Der ständige technologische Wandel bringt stets potenzielle Risiken mit sich. Daher stehen Verbraucher und insbesondere Verbraucherverbände der RFID-Technologie z. T. kritisch gegenüber, da sie Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung befürchten. Die Untersuchung hat jedoch gezeigt, dass das deutsche Datenschutz- und Datensicherheitsrecht durch ein besonders hohes Schutzniveau geprägt ist. In Anbetracht dieser umfassenden Normierung ist eine zusätzliche gesetzliche Regelung für die RFID-Technologie nicht erforderlich. Vielmehr ist die Verantwortung der Handelnden für einen sozialverträglichen Einsatz gefordert. Um den Vorbehalten gegen RFID zu begegnen, sollten Vorkehrungen getroffen werden, die über das bestehende gesetzlich festgelegte Schutzniveau hinausgehen. So bietet sich die Selbstverpflichtung von betroffenen Unternehmen zur Umsetzung von Hinweispflichten bzw. Kennzeichnung von Produkten an, die mit RFID-Tags ausgestattet sind, so wie dies auch im Rahmen der Selbstverpflichtungserklärung von EPCglobal der Fall ist. Den Verbrauchern sollten Auskunftsrechte in Bezug auf die gespeicherten Daten gewährt werden, auch wenn es sich nicht um personenbezogene Daten handelt. Ferner sollte den Verbrauchern die Möglichkeit zur Deaktivierung von RFID-Tags eingeräumt werden. Durch ein Auditierungsverfahren könnte ein freiwilliges Managementsystem zum Schutz persönlicher Daten, der Datensicherheit oder des Fernmeldegeheimnisses eingeführt werden. Auch Gütesiegel können dazu beitragen, das Vertrauen der Verbraucher zu stärken, da sie so selbst beurteilen können, wie ein Unternehmen mit den Themen Datenschutz und -sicherheit umgeht.

Eine neue Relevanz des Datenschutzes ergibt sich aus dem Risiko des ungezielten Datenempfangs bei der automatischen Identifikation in der Alltagsanwendung. Da die Möglichkeiten hier aber noch zu unbestimmt sind, macht es keinen Sinn, darauf mit einer eigenen gesetzlichen Regelung zu reagieren. Das Datenschutzrecht ist flexibel genug, um diesen neuen Herausforderungen gerecht zu werden.



LITERATURVERZEICHNIS UND
INTERNETDOKUMENTE

LITERATURVERZEICHNIS

Bergmann, Lutz/Möhrle, Roland/Herb, Armin

Datenschutzrecht, Kommentar zum Bundesdatenschutzgesetz, den Datenschutzgesetzen der Länder und zum Bereichsspezifischen Datenschutz, Loseblattsammlung, Stuttgart, Stand: September 2005

Conrad, Isabell

RFID-Ticketing aus datenschutzrechtlicher Sicht, Eine Untersuchung datenschutzrechtlicher Grenzen am Beispiel des Einsatzes in Tickets zur FIFA Fußball WM 2006, in: CR 2005, 537 ff.

Finkenzeller, Klaus

RFID-Handbuch, Grundlagen und Praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten, 3. Aufl., München 2003

Gola, Peter/Schomerus, Rudolf

BDSG, Bundesdatenschutzgesetz, Kommentar, 8. Aufl., München 2005

Hilgendorf, Eric

Grundfälle zum Computerstrafrecht, Teil 2: Die Computerspionage, in: JuS 1996, 702 ff.

ders.

Grundfälle zum Computerstrafrecht, Teil 3: Die Datenveränderung, in: JuS 1996, 890 ff.

ders.

Grundfälle zum Computerstrafrecht, Teil 4: Die Computersabotage, in: JuS 1996, 1082 ff.

Holznagel, Bernd/Bonnekoh, Mareike

Radio Frequency Identification – Innovation vs. Datenschutz?, in: MMR 2006, 17 ff.

Jeschek, Hans-Heinrich/Ruß, Wolfgang/Willms, Günther (Hrsg.)

Strafgesetzbuch, Leipziger Kommentar, Großkommentar, 10. Aufl., Berlin, New York 1989

Fünfter Band: §§ 185–262

Siebter Band: §§ 303–358

Kelter, Harald/Wittmann, Stefan

Radio Frequency Identification - RFID, Chancen und Risiken des RFID-Einsatzes, in: DuD 2004, 331 ff.

Kilian, Wolfgang/Heussen, Benno

Computerrechts-Handbuch, Loseblattsammlung, München, Stand: März 2005

Klußmann, Niels

Lexikon der Kommunikations- und Informationstechnik, 3. Aufl., Heidelberg 2001

Lackner, Karl/Kühl, Kristian

Strafgesetzbuch mit Erläuterungen, 25. Aufl., München 2004

Lahner, Claus Mauricio

Datenschutzrechtliche Probleme beim Einsatz von RFID-Systemen, Hannover 2004

Langheinrich, Marc

Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie, Zürich 2004

Leckner, Theodor/Winkelbauer, Wolfgang

Computerkriminalität – Möglichkeiten und Grenzen des 2. WiKG (III), in: CR 1986, 824 ff.

Möhrenschlager, Manfred

Das neue Computerstrafrecht, in: wistra 1986, 128 ff.

Müller, Jürgen

Ist das Auslesen von RFID-Tags zulässig? Schutz von RFID-Transponderinformationen durch § 86 TKG, in: DuD 2004, 215 ff.

Neumann, Ulfried/Puppe, Ingeborg/Schild, Wolfgang (Gesamtredaktion)

Nomos-Kommentar zum Strafgesetzbuch, 1.–14. Lieferung, Baden-Baden 2004

Palandt, Otto

Bürgerliches Gesetzbuch, Kurzkomentar, 65. Aufl., München 2006

Rankl, Wolfgang/Effing, Wolfgang

Handbuch der Chipkarten, 4. Aufl., München, Wien 2002

Roßnagel, Alexander

Ubiquitous Computing – neue Herausforderungen für den Datenschutz, Ein Paradigmenwechsel und die von ihm betroffenen normativen Ansätze, in: CR 2004, 625 ff.

ders.

Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003

ders.

Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, in: MMR 2005, 71 ff.

Säcker, Franz Jürgen

Berliner Kommentar zum Telekommunikationsgesetz, Frankfurt am Main 2006

Schaar, Peter

Überwachung des Bürgers durch Staat und Wirtschaft – Welche Perspektiven hat der Datenschutz?, in: RDV, Sonderbeilage zu Heft 1/2005, 1 ff.

Schaffland, Hans-Jürgen/Wiltfang, Noeme

Bundesdatenschutzgesetz, Kommentar, Loseblattsammlung, Berlin, Stand: 2005

Scheurle, Klaus-Dieter/Mayen, Thomas

Telekommunikationsgesetz, Kommentar, München 2002

Schmitz, Roland

Ausspähen von Daten, § 202a StGB, in: JA 1995, 478 ff.

Schönke, Adolf/Schröder, Horst

Strafgesetzbuch, Kommentar, 27. Aufl., München 2006

Schulze-Heiming, Ingeborg

Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls, Diss., Münster 1995

Simitis, Spiros

Kommentar zum Bundesdatenschutzgesetz, 5. Aufl., Baden-Baden 2003

Tinnefeld, Marie-Theres/Ehmann, Eugen/Gerlin, Rainer W.

Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheit in europäischer Sicht, 4. Aufl., München, Wien 2005

Weichert, Thilo

Datenschutzrechtliche Anforderungen an Chipkarten, in: DuD 1997, 266 ff.

Weis, Stephen A.

Security and Privacy in Radio-Frequency Identification Devices, Cambridge 2003

ders./Sarma, Sanjay E./Rivest, Ronald L./Engels, Daniel W.

Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, Cambridge 2003

Westerholt, Margot Gräfin von/Döring, Wolfgang

Datenschutzrechtliche Aspekte der Radio Frequency Identification. Ein „Virtueller Rundgang“ durch den Supermarkt der Zukunft, in: CR 2004, 710 ff.

INTERNETDOKUMENTE

A. T. Kearny

„RFID spart dem deutschen Einzelhandel sechs Milliarden Euro pro Jahr. Nutzen für Händler – Kosten für Hersteller“, Pressemitteilung vom 08. März 2004, abrufbar über die Homepage der Unternehmensberatung <<http://www.atkearny.de>>

Association for Automatic Identification and Mobility (AIM)

What is Frequency Identification (RFID)?, 2004, <http://www.aimglobal.org/technologies/rfid/what_is_rfid.asp>

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Risiken und Chancen des Einsatzes von RFID-Systemen, Studie, 2004, <<http://www.bsi.de/fachthem/rfid/RIKCHA.pdf>>

Finke, Thomas/Kelter, Harald

Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO 14443-Systems, <http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf>

Hascher, Wolfgang

Identifikation mit Mini-Chips, Elektronik-Heft 19, 2003, <<http://www.elektroniknet.de/topics/kommunikation/fachthemen/2003/0021/index.htm>>

Landt, Jeremy

Shrouds of Time, The History of RFID, 2001, <http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf>

Schaar, Peter

„Überwachung im Alltag ist jetzt möglich“, Interview in der Berliner Zeitung vom 6. Januar 2006; abrufbar unter <<http://www.berlinonline.de/berliner-zeitung/politik/515174.html?2006-01-06>>

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Kundenbindungssysteme und Datenschutz, 2003, S. 69; abrufbar über <http://www.vzbv.de/mediapics/kundenbindungssysteme_kurzfassung_2003.pdf>

Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. (FoeBud)

Positionspapier über den Gebrauch von RFID auf und in Konsumgütern, <<http://www.foebud.org/rfid/positionspapier.pdf>>

Wikipedia, Freie Enzyklopädie

Stichwort: Radio Frequency Identification, <<http://de.wikipedia.org/wiki/Rfid>>

INFORMATIONSFORUM **RFID** 

INFORMATIONSFORUM RFID e.V.

Dorotheenstraße 37
10117 Berlin
Tel. +49 (0) 30.206581-0
Fax +49 (0) 30.206581-20

info@info-rfid.de
www@info-rfid.de